# Operations Department (OD) — Complete SOP Set

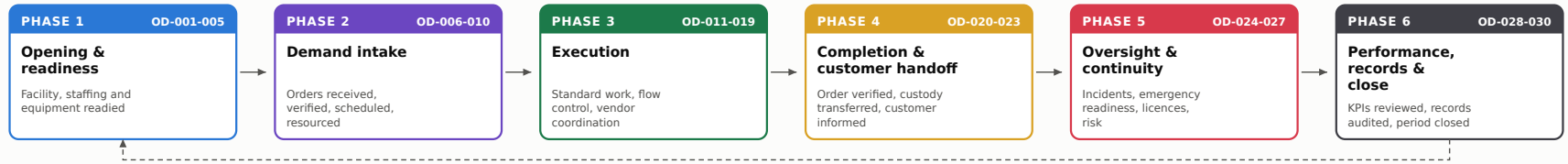
## Archetype: DATA_HOSTING · Data Hosting

Tier: Free (entire Operations department) · Modules: 30 · Standard: locked 13-section

## Contents



FIGURE 1 — OPERATIONS WORKFLOW




Six phases · 30 modules · one continuous operating cycle, closing back into Phase 1 the next operating day.

# Modules

- OD-001 — Daily Operations Opening Procedure
- OD-002 — Shift Handover & Briefing
- OD-003 — Staffing & Coverage Verification
- OD-004 — Work Area Readiness & Housekeeping Inspection
- OD-005 — Operational Equipment Availability Check
- OD-006 — Customer Order / Work Request Intake
- OD-007 — Order Verification & Acceptance Review
- OD-008 — Job Scheduling & Sequencing
- OD-009 — Resource & Capacity Allocation
- OD-010 — Incoming Material / Supply Verification
- OD-011 — Standard Work Execution & Process Adherence
- OD-012 — Work-in-Progress Tracking & Status Update
- OD-013 — Operational Handoff Between Work Stages
- OD-014 — Output Monitoring & Throughput Review
- OD-015 — Bottleneck Identification & Response
- OD-016 — Rework & Nonconforming Work Handling
- OD-017 — Schedule Deviation & Change Management
- OD-018 — Subcontractor & Vendor Coordination
- OD-019 — Interdepartmental Coordination Review
- OD-020 — Job / Order Completion Verification
- OD-021 — Delivery / Service Turnover
- OD-022 — Customer Communication & Status Notification
- OD-023 — Customer Feedback & Complaint Intake
- OD-024 — Operational Incident Reporting & Response
- OD-025 — Emergency & Business Continuity Readiness Check
- OD-026 — Regulatory, License & Permit Currency Verification
- OD-027 — Operational Risk Review
- OD-028 — Operational KPI Review
- OD-029 — Operational Records Retention & Documentation Audit
- OD-030 — End-of-Shift / End-of-Day Operations Closeout

# Phase 1 — Opening & readiness

## OD-001 — Daily Operations Opening Procedure

**Estimated completion time: 30–60 minutes per shift**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

### 1. Purpose

This procedure establishes the standardized start-of-shift readiness sequence for a data hosting facility, ensuring the incoming operations shift confirms environmental, network, and monitoring status and formally signs on before customer-facing hosting work begins. It protects service continuity and SLA compliance from the first minute of the shift.

### 2. Scope

Covers the facility/shift start-up sequence, control-room readiness verification, monitoring-console confirmation, and the operator sign-on handoff at the beginning of each operations shift. Excludes work-area housekeeping (see OD-004), equipment availability confirmation (see OD-005), and safety-specific readiness (see SD-001).

### 3. Responsibilities

- Shift Operations Lead (Data Center Operator I/II) — executes the opening sequence, confirms console and environmental status, and completes the sign-on log.
- Network Operations Center (NOC) Technician — verifies network reachability, monitoring dashboards, and alarm-queue status for incoming shift.
- Operations Shift Supervisor — reviews the outgoing-shift handoff notes, authorizes shift sign-on, and verifies the completed checklist.

### 4. Required PPE & Lockout/Tagout

- Standard facility PPE (access badge, ESD wrist strap when entering raised-floor or rack areas); no additional PPE required for control-room sign-on activity.
- Not applicable — no hazardous energy is manipulated during this administrative opening procedure.

### 5. Regulatory References

- None sector-specific to the opening sign-on task; internal Operations Policy OD-POL-01 applies. Related governing frameworks include SOC 2 (AICPA TSC) availability criteria and, where applicable, ISO/IEC 27001 operational monitoring controls and customer contractual SLAs.

- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow


## 7. Step-by-Step Procedure

1. Receive the outgoing shift's handoff notes; review open tickets, in-progress maintenance windows, and any deferred alarms.
2. Confirm facility environmental status on the BMS/DCIM dashboard — temperature, humidity, and airflow readings within customer-committed operating envelope (defer equipment availability specifics to OD-005).
3. Confirm power status indicators — utility feed, UPS charge state, and generator "ready" status show nominal on the monitoring console.
4. Verify all monitoring and alerting consoles are live: NOC dashboards streaming, no stale data feeds, and the alarm queue reconciled to zero unacknowledged criticals.
5. Confirm network edge reachability — validate uptime probes and external circuit status for primary and redundant links.
6. Confirm the overnight backup and replication jobs reported success; note any failures for escalation before shift start.
7. Complete the shift sign-on log: record operator names, timestamp, console status, and any carried-over items; obtain Supervisor authorization.
8. Document the completed opening checklist and file it in the shift-log repository for the audit trail.

## 8. Decision Tree

OD-001 · OPERATIONS · DATA HOSTING

## Decision Tree — Daily Operations Opening Procedure

START — THIS PROCEDURE ESTABLISHES THE STANDARDIZED START-OF-SHIFT READINESS SEQUENCE FOR A DATA HOSTING FACILITY, ENSURING THE INCOMING OPERATIONS SHIFT CONFIRMS ENVIRONMENTAL, NETWORK, AND MONITORING …

**Issue identified during this procedure?**

- **NO** → **Complete the checklist and close out the procedure**
  END — NO FINDING, ACTIVITY CONTINUES
- **YES** → **Classify severity**
  Assign the highest severity that applies — not the first that matches.

### MINOR

**DEFINITION**
no safety, compliance, or service impact

**ACTION**
Log in the shift-sign-on notes, flag for follow-up, and continue sign-on

**ESCALATE TO**
No escalation — handled at task level

*Timing: resolve in the moment; work proceeds*

### MAJOR

**DEFINITION**
material risk to safety, compliance, output, or service — not an immediate hazard

**ACTION**
Hold shift sign-on for the affected function, escalate to the Operations Shift Supervisor, and resolve before declaring the shift ready

**ESCALATE TO**
Operations Shift Supervisor

*Timing: resolve before the work proceeds*

### CRITICAL

**DEFINITION**
a customer-impacting outage or SLA breach condition present at shift start (e.g., unacknowledged critical alarm, failed environmental envelope, or dark monitoring console)

**ACTION**
Do not sign on as ready; immediately notify the Operations Shift Supervisor and NOC on-call, invoke incident response, and retain outgoing shift until stabilized

**ESCALATE TO**
Supervisor

*Timing: immediate — halts the activity*

**Record the finding, the action taken, and the verification**
Close the item only once the corrective action is verified and the record is complete.

**ACTIVITY RELEASED / CLOSED**

### READING THIS TREE

- **No finding** — Activity stands. Complete the checklist and continue.
- **Minor** — Handled in place at task level; no escalation.
- **Major** — Supervisory decision required before the next stage.
- **Critical** — Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- Outgoing-shift handoff reviewed and all open critical items acknowledged.
- Environmental and power dashboards confirmed within committed envelope.
- All monitoring consoles live with alarm queue reconciled.
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| Outgoing-shift handoff notes reviewed and acknowledged | | |
| BMS/DCIM environmental readings within envelope | | |
| Power status (utility, UPS, generator) nominal | | |
| Monitoring consoles live; alarm queue reconciled | | |
| Network edge reachability confirmed (primary + redundant) | | |
| Overnight backup/replication jobs verified successful | | |
| Shift sign-on log completed and authorized | | |

## 11. KPIs

- Opening procedure completed before shift start time: 100% of shifts.
- Sign-on log completeness (all fields recorded and authorized): ≥ 99%.
- Critical readiness issues caught at opening vs. surfaced mid-shift: ≥ 95% caught at opening.

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# OD-002 — Shift Handover & Briefing

**Estimated completion time: 20–40 minutes per handover**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

To ensure continuous, accountable operation of the data center floor and Network Operations Center (NOC) by transferring an accurate, structured account of infrastructure status, open incidents, and shift priorities from the outgoing to the incoming operations crew.

## 2. Scope

Covers the structured outgoing→incoming handover of hosting/facility status, open tickets, active change windows, and prioritized watch items for NOC and floor operations staff. Excludes the safety pre-shift briefing (see SD-003) and maintenance-crew handover (see MD-001), which are authored in their own modules.

## 3. Responsibilities

- Outgoing Shift Lead (NOC) — compiles and presents the handover record; owns accuracy of all open-issue status until transfer is acknowledged.
- Incoming Shift Lead (NOC) — reviews, questions, and formally accepts the handover; assumes ownership of priorities at transfer.
- Operations Supervisor — verifies handover completeness, arbitrates disputed items, and signs off on the handover record.

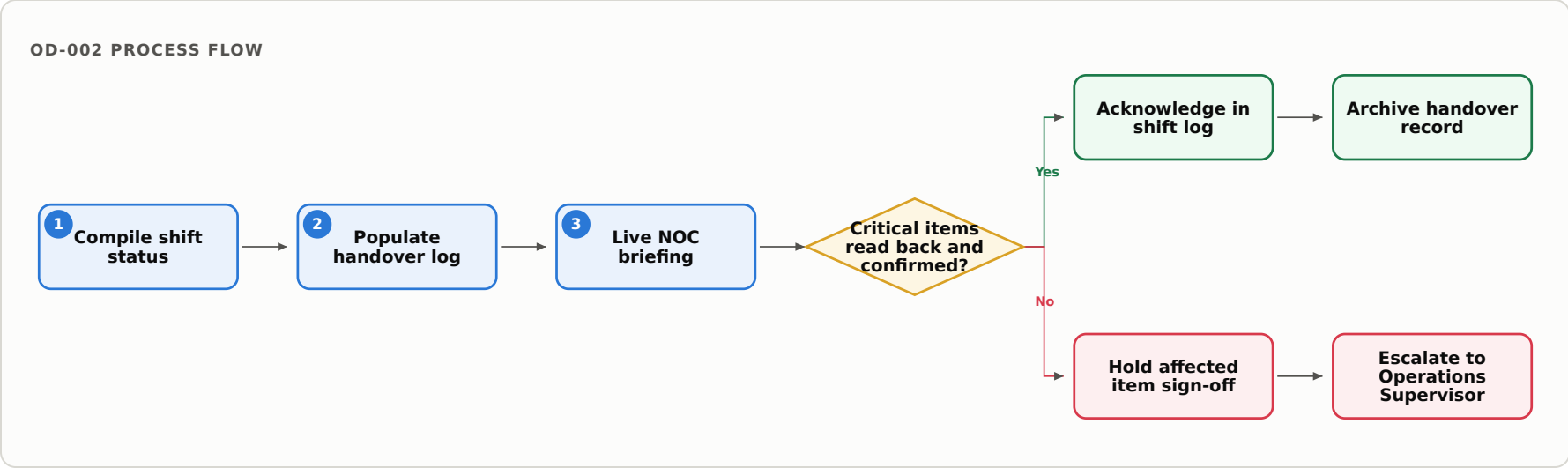
## 4. Required PPE & Lockout/Tagout

- Standard facility PPE (badge/access credential, ESD-safe practices when on the raised floor); handover itself is performed in the NOC.
- Not applicable — no hazardous energy involved; this is an administrative coordination task.

## 5. Regulatory References

- None sector-specific mandatory for handover briefing; internal NOC operating policy applies. Supporting frameworks: SOC 2 (AICPA TSC) availability/change-management criteria and ISO/IEC 27001:2022 A.5.24 (incident management) inform record content.
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow



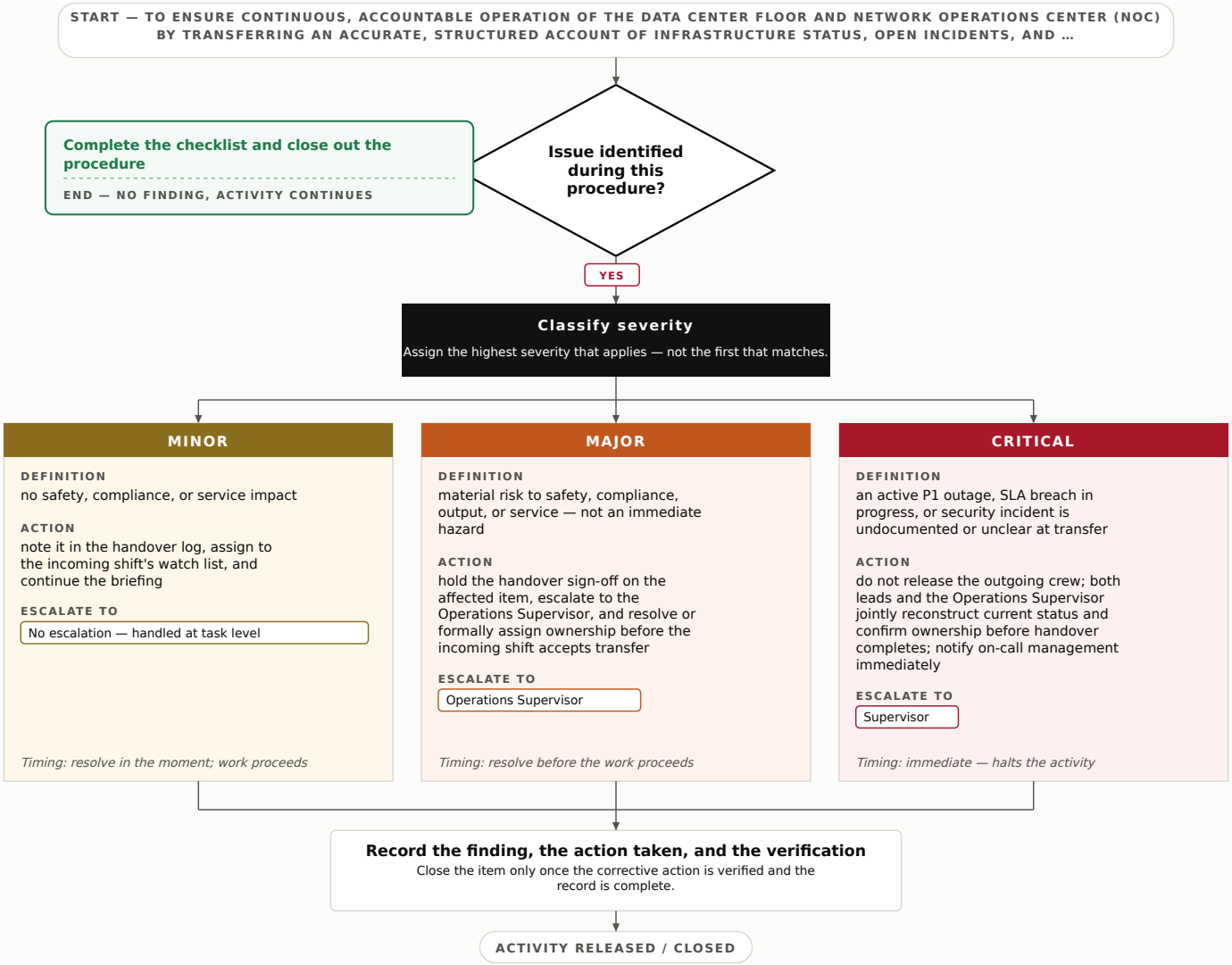

## 7. Step-by-Step Procedure

1. Outgoing Shift Lead reviews the DCIM dashboard, alarm queue, and open ticket board; captures power/cooling/environmental status, capacity flags, and network health.
2. Record all open and in-progress incidents by ticket ID, severity, affected customer/tenant, current status, and next required action.
3. List active or pending change windows, maintenance activities in progress, and any change-freeze in effect (hand-off to MD-001 acknowledged where floor work continues across shifts).
4. Flag customer SLA commitments at risk (response/resolution clocks) and any pending customer communications owed within the incoming shift.
5. Conduct the live handover briefing at the NOC with both leads present; walk the incoming lead through each open item and the ranked priority list.
6. Incoming Shift Lead reads back critical items and confirms understanding; unresolved questions are resolved before transfer, not after.
7. Both leads acknowledge the handover in the shift log; ownership of all open items transfers to the incoming shift at acknowledgment.
8. Archive the completed handover record to the shift log repository and notify the Operations Supervisor for verification.

## 8. Decision Tree

OD-002 · OPERATIONS · DATA HOSTING

## Decision Tree — Shift Handover & Briefing




READING THIS TREE

**No finding**
Activity stands. Complete the checklist and continue.

**Minor**
Handled in place at task level; no escalation.

**Major**
Supervisory decision required before the next stage.

**Critical**
Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- Every open ticket carries a ticket ID, severity, and defined next action at transfer.
- All at-risk SLA clocks and owed customer communications are explicitly named to the incoming lead.
- Critical items received a verbal read-back and confirmation from the incoming Shift Lead.
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| DCIM/environmental status reviewed and logged | | |
| All open incidents recorded with ID, severity, next action | | |
| Active/pending change windows and any change-freeze noted | | |
| At-risk SLA clocks and owed customer comms flagged | | |
| Live briefing conducted with both leads present | | |
| Critical items read back and confirmed by incoming lead | | |
| Handover acknowledged in shift log and archived | | |

## 11. KPIs

- Handover record completeness (all fields populated): ≥ 98%
- Open items dropped or lost across shift transitions: 0
- On-time handover start (within 15 min of shift boundary): ≥ 95%

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# OD-003 — Staffing & Coverage Verification

**Estimated completion time: 20–40 minutes per shift handover**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

To confirm that every required Operations role for the data center operating period — NOC operators, facilities/DCIM technicians, and on-call escalation leads — is physically present, credentialed, and assigned before the shift assumes control, protecting uptime and incident-response readiness.

## 2. Scope

Covers pre-shift verification that mandated roles are staffed, current on required credentials, and formally assigned to a coverage position for the operating period at the hosting facility. Excludes schedule and shift assignment, which is covered under HR-015, and staff competency assessment, which is covered under TR-020.

## 3. Responsibilities

- Shift Operations Lead (NOC) — runs the coverage verification, confirms present-and-assigned status, and authorizes shift takeover.
- Facilities Operations Supervisor — confirms critical-facilities (power/cooling/DCIM) coverage and on-call availability.
- Data Center Manager — resolves coverage gaps, approves minimum-staffing exceptions, and signs off.

## 4. Required PPE & Lockout/Tagout

- Standard facility PPE — badge/access credential and ESD-safe footwear where entering white-space; no additional PPE for the verification itself.
- Not applicable — no hazardous energy involved in this administrative verification.

## 5. Regulatory References

- None sector-specific mandate staffing counts; internal policy applies. Related frameworks used as basis: SOC 2 (Trust Services Criteria — Availability/Common Criteria) and ISO/IEC 27001 Annex A operational controls; Uptime Institute Tier operational-sustainability staffing guidance; OSHA 29 CFR 1910 general recordkeeping for on-site personnel.
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow

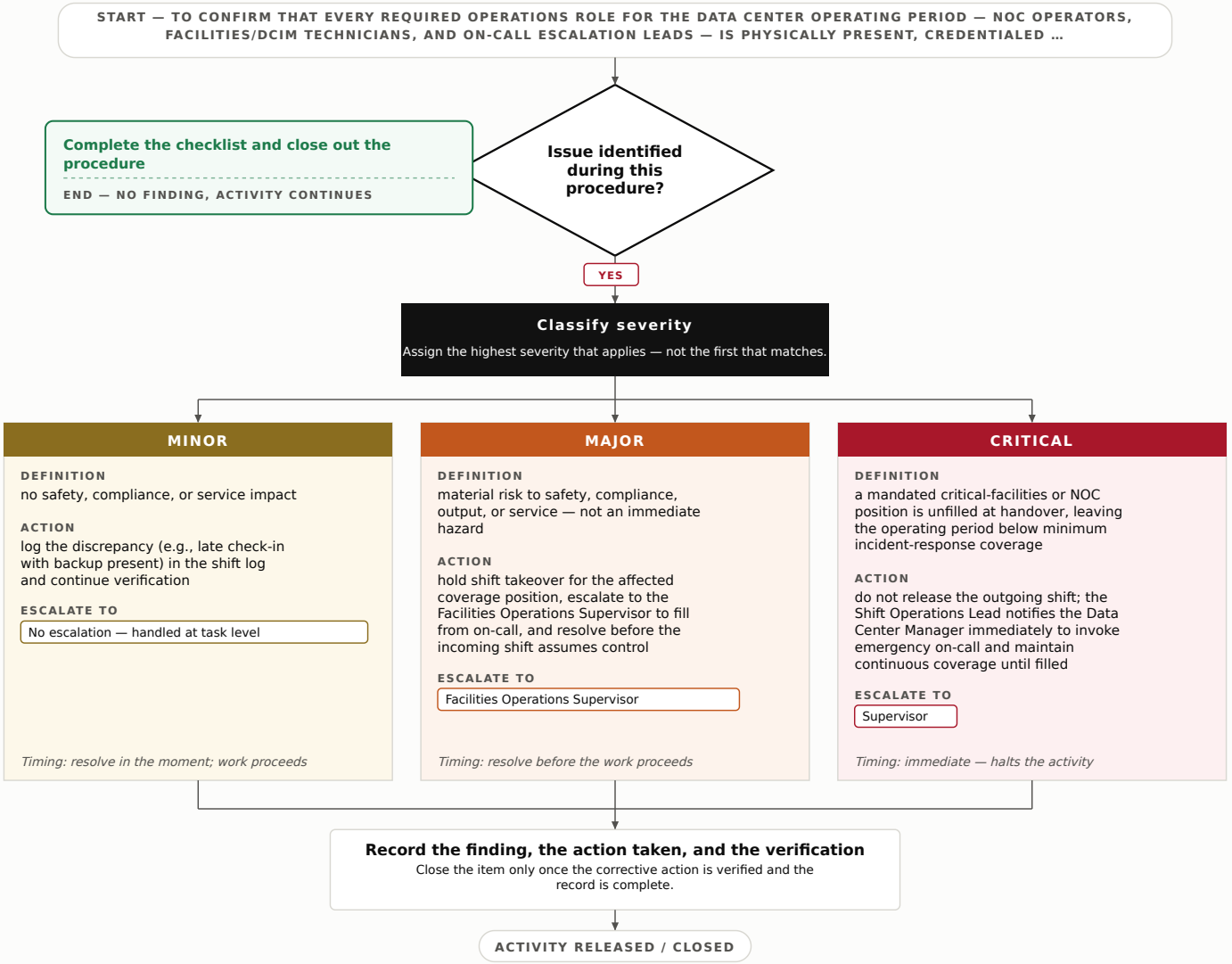

## 7. Step-by-Step Procedure

1. Retrieve the required-role coverage matrix for the operating period from the DCIM/shift board (minimum NOC operators, facilities technicians, security escort, and on-call escalation lead).
2. Confirm each named person has checked in — badge-in log for on-site roles, presence acknowledgment for remote/on-call roles — and note actual headcount against minimum.
3. Verify each role holder's site access credential is active and not expired or suspended (badge system status).
4. Confirm required incident-response and vendor-escort authorizations are current; where competency is a prerequisite, confirm status per TR-020 (do not reassess here).
5. Match every open coverage position (NOC console, critical-facilities on-call, escalation lead) to an assigned, present, credentialed individual; flag any unfilled or double-booked position.
6. For any gap, contact the Facilities Operations Supervisor / Data Center Manager to fill from on-call before takeover; log the action taken.
7. Confirm outgoing shift has completed handover of open incidents/tickets to the assigned incoming role holders.
8. Record verification result (roles required, present, assigned, gaps/resolutions) in the shift log and authorize shift takeover.

## 8. Decision Tree

OD-003 · OPERATIONS · DATA HOSTING

## Decision Tree — Staffing & Coverage Verification




READING THIS TREE

- **No finding** — Activity stands. Complete the checklist and continue.
- **Minor** — Handled in place at task level; no escalation.
- **Major** — Supervisory decision required before the next stage.
- **Critical** — Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- Actual present headcount meets or exceeds documented minimum for every required role.
- All assigned role holders hold active, unexpired site access credentials.
- Every coverage position is mapped to exactly one present, credentialed individual (no gaps, no double-booking).
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| Required-role coverage matrix retrieved for operating period | | |
| Actual headcount meets minimum per role | | |
| All role holders checked in (badge/on-call acknowledgment) | | |
| Site access credentials active for all assigned staff | | |
| Each coverage position assigned to one present individual | | |
| Coverage gaps filled or exception approved by Data Center Manager | | |
| Open-incident handover to incoming roles confirmed | | |

## 11. KPIs

- Shifts starting at or above minimum coverage: ≥ 99%.
- Coverage-verification completed before scheduled takeover time: 100%.
- Unresolved critical coverage gaps at handover: 0 per quarter.

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# OD-004 — Work Area Readiness & Housekeeping Inspection

**Estimated completion time: 30–45 minutes per shift start**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

Ensure data hall floors, operator workstations, staging zones, and hot/cold aisles are clear, organized, and fit for the day's operations so that airflow, egress, and technician safety are preserved before any rack work, cabling, or maintenance activity begins.

## 2. Scope

Covers pre-shift readiness and housekeeping inspection of raised-floor data halls, operator NOC workstations, equipment staging/kitting areas, and aisle containment within the Operations footprint. Excludes warehouse/receiving-dock housekeeping (see WH-023) and maintenance-shop housekeeping (see MD-025).

## 3. Responsibilities

- Data Center Operations Technician — Performs the walk-through, clears debris and trip hazards, verifies aisle and floor readiness, records findings on the checklist.
- Operations Shift Lead — Reviews completed checklist, classifies escalated findings, holds affected zones and dispatches corrections.
- Facilities Operations Manager — Owns the procedure, resolves Critical findings, authorizes zone release for operations.

## 4. Required PPE & Lockout/Tagout

- Standard facility PPE: closed-toe non-slip footwear, ESD wrist strap/heel straps when handling exposed hardware, hi-vis vest in active staging zones.
- Not applicable — no hazardous energy is de-energized during inspection. Do not open, tag, or de-energize live PDUs, busways, or racks; report electrical hazards to Facilities per Section 8.

## 5. Regulatory References

- 29 CFR 1910.22 (Walking-Working Surfaces — housekeeping, clearances, trip hazards)
- 29 CFR 1910.37 (Maintenance and access of exit routes / egress)
- NFPA 75 (Fire Protection of Information Technology Equipment — aisle clearance and combustible control)
- ASHRAE TC 9.9 thermal-containment guidance (aisle airflow integrity)
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow

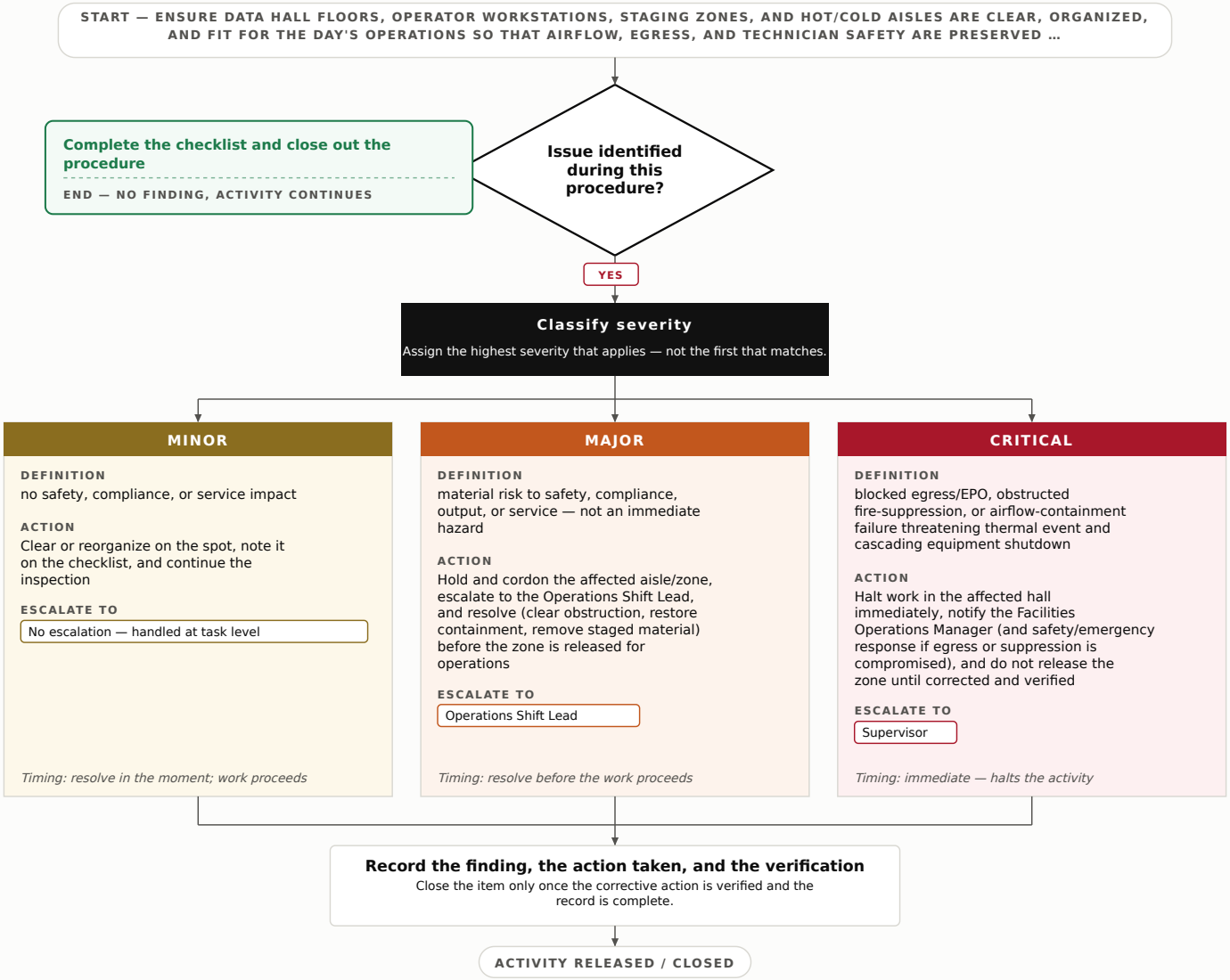

## 7. Step-by-Step Procedure

1. Collect the shift checklist and confirm which data halls, aisles, and staging zones are in scope for the day's work orders.
2. Inspect raised-floor aisles and walkways for debris, packaging, loose cabling, and displaced floor tiles; confirm no obstructions to egress routes or emergency exits.
3. Verify hot/cold aisle containment doors/panels are closed and unobstructed and that no boxes or carts block airflow perforated tiles.
4. Inspect operator NOC workstations for cleanliness, cable tidiness, and removal of food/liquids away from equipment.
5. Check equipment staging/kitting areas — inbound hardware from suppliers (334111/334112) must be stored on designated racks or carts, not on floors or in aisles.
6. Confirm fire-suppression clearances, extinguishers, and EPO stations are visible, unblocked, and access-clear per NFPA 75.
7. Clear minor debris and organize as found; flag and escalate any hazard that cannot be immediately corrected per the Decision Tree.
8. Record all findings, corrections, and zone status on the Inspection Checklist and route to the Operations Shift Lead for sign-off.

## 8. Decision Tree

OD-004 · OPERATIONS · DATA HOSTING

## Decision Tree — Work Area Readiness & Housekeeping Inspection




READING THIS TREE

- **No finding** — Activity stands. Complete the checklist and continue.
- **Minor** — Handled in place at task level; no escalation.
- **Major** — Supervisory decision required before the next stage.
- **Critical** — Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- All in-scope egress routes, EPO stations, and fire-suppression access confirmed clear.
- Hot/cold aisle containment intact and airflow tiles unobstructed.
- Staging areas organized; no hardware or packaging left in aisles or walkways.
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| Data hall aisles/walkways clear of debris and trip hazards | | |
| Egress routes and emergency exits unobstructed | | |
| Hot/cold aisle containment closed; airflow tiles unblocked | | |
| NOC workstations clean, cabling tidy, no liquids near equipment | | |
| Staging/kitting area organized; inbound hardware racked, not floored | | |
| Fire-suppression, extinguishers, EPO stations visible and clear | | |
| No displaced or lifted raised-floor tiles | | |

## 11. KPIs

- Pre-shift inspection completion rate: 100% of scheduled shifts.
- Unresolved Critical findings at zone release: 0.
- Repeat housekeeping findings in same zone within 7 days: ≤ 5%.

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# OD-005 — Operational Equipment Availability Check

**Estimated completion time: 30–60 minutes per shift/period**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

This procedure confirms that the equipment and tools required for the operating period — production and spare servers, storage arrays, network switches, KVM/crash carts, and provisioning media — are physically present, powered/functional, and released for use so hosting operations can proceed without avoidable interruption to customer workloads.

## 2. Scope

Covers the availability, presence-count, and release-for-use verification of Operations equipment and tools staged for the current period across production floor and staging areas. Excludes equipment condition/inspection (see ED-003), preventive-maintenance status (see PM-024), and materials-handling-equipment pre-use checks (see WH-004).

## 3. Responsibilities

- Operations Shift Lead (OD) — owns the availability check, confirms release-for-use, signs off before the period begins.
- Data Center Technician (OD) — physically verifies presence, power state, and connectivity of listed equipment and reports discrepancies.
- Inventory/Provisioning Coordinator (OD) — maintains the equipment/spares register and reconciles counts against upstream receipts.

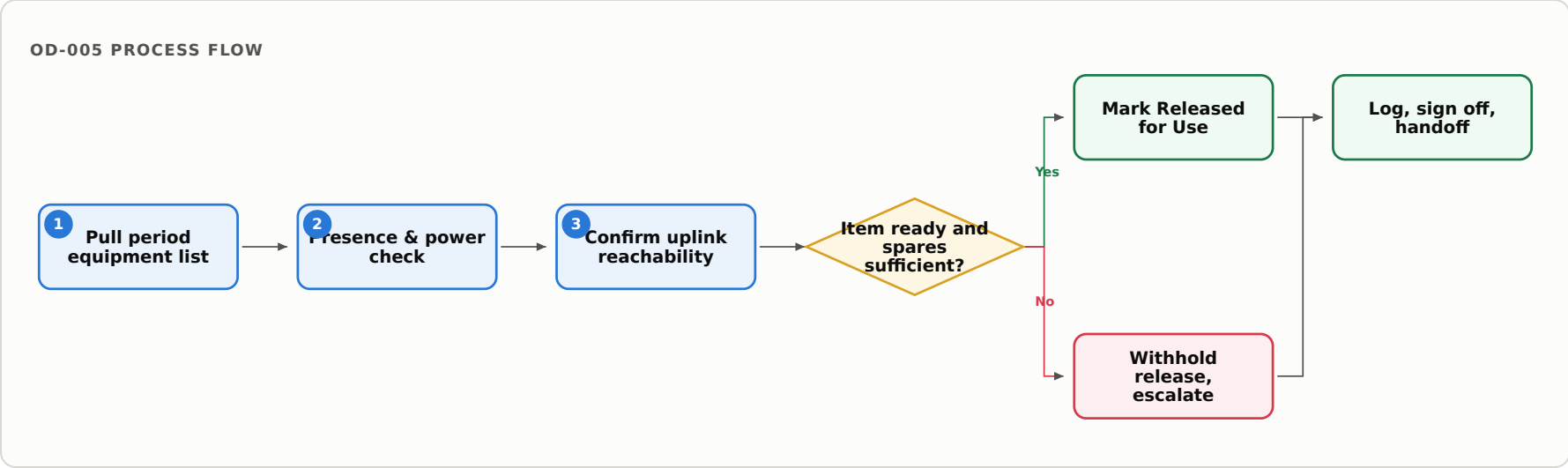
## 4. Required PPE & Lockout/Tagout

- Standard facility PPE: ESD wrist strap when handling drives/boards, closed-toe footwear on the raised floor.
- Not applicable — no hazardous energy work performed in this task; energized-work and isolation belong to maintenance procedures.

## 5. Regulatory References

- OSHA 29 CFR 1910.303–.305 (general electrical/wiring for equipment in service — presence of energized racks); NFPA 75 (Standard for the Fire Protection of Information Technology Equipment); internal Operations Availability & Spares Policy (OD-POL-02) for release-for-use thresholds. No hosting-specific federal equipment-availability standard applies.
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow



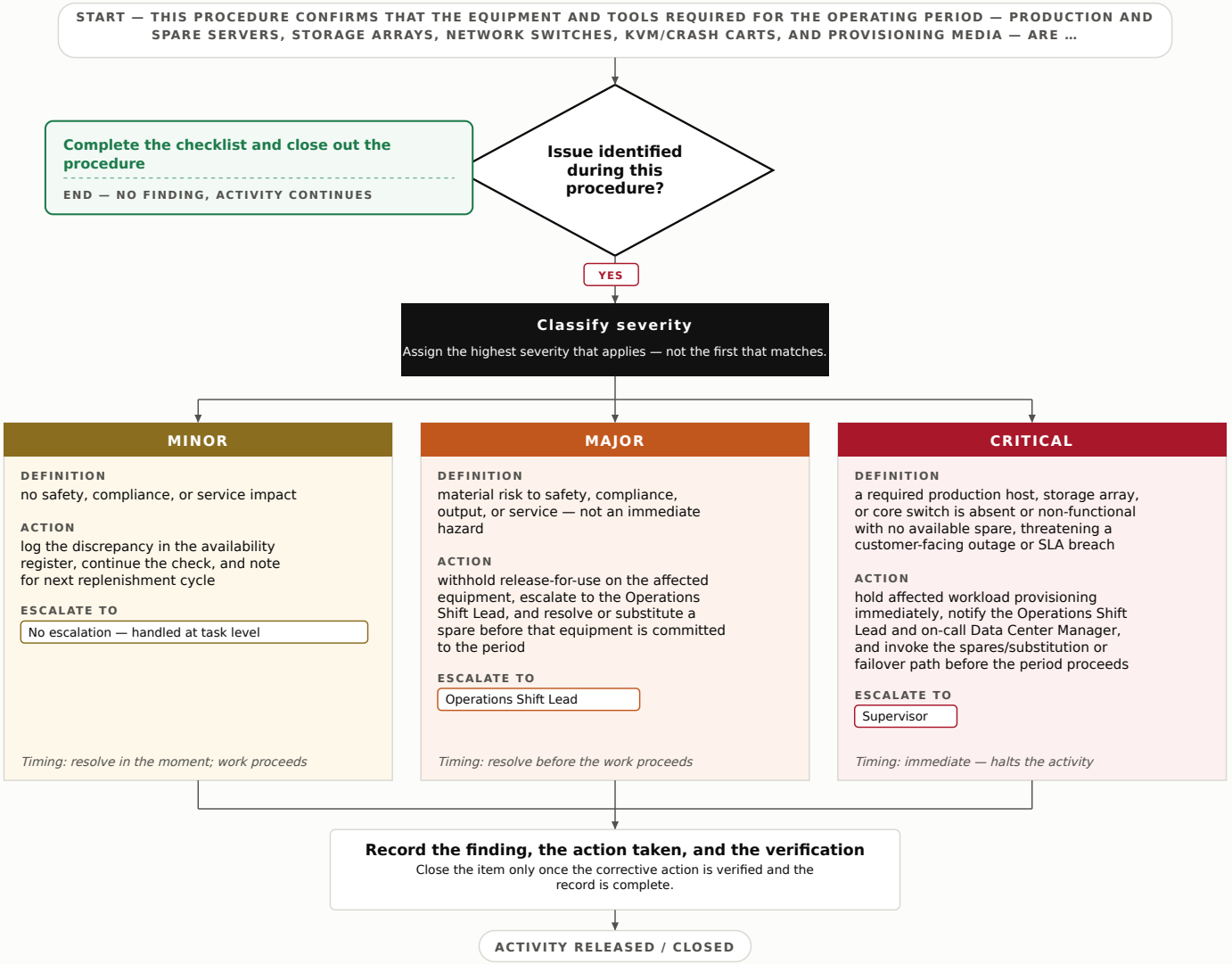

## 7. Step-by-Step Procedure

1. Retrieve the period equipment/tools list and spares register from the Inventory/Provisioning Coordinator; confirm it matches the day's workload and provisioning schedule.
2. Walk the production floor and staging area; confirm each listed unit (servers, storage arrays, switches, KVM/crash cart, provisioning media) is physically present at its assigned location.
3. Verify each unit's power/standby state and indicator status shows ready — powered, linked, and not in an active fault-hold from another procedure.
4. Confirm network/uplink connectivity and management-plane reachability for units required to be online this period; note any unreachable device.
5. Reconcile spare-drive, spare-PSU, and cable/optic counts against the register; flag any shortfall below the OD-POL-02 minimum stocking threshold.
6. Mark each verified item "Released for Use"; withhold release on any item that is missing, unpowered, unreachable, or below spares minimum.
7. Route any condition or maintenance-status concerns to the correct owner (ED-003 / PM-024) — do not adjudicate them here.
8. Record results on the Inspection Checklist, log discrepancies, and obtain Shift Lead sign-off before the period begins.

## 8. Decision Tree

OD-005 · OPERATIONS · DATA HOSTING

## Decision Tree — Operational Equipment Availability Check




READING THIS TREE

- **No finding** — Activity stands. Complete the checklist and continue.
- **Minor** — Handled in place at task level; no escalation.
- **Major** — Supervisory decision required before the next stage.
- **Critical** — Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- Every item on the period list is accounted for as present or explicitly flagged missing.
- Spare counts meet or exceed OD-POL-02 minimum stocking thresholds.
- All released equipment is powered, reachable, and free of active fault-holds.
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| Period equipment/tools list retrieved and matched to workload | | |
| All production servers/hosts present at assigned locations | | |
| Storage arrays present, powered, and management-reachable | | |
| Core/access switches and uplinks connected and linked | | |
| KVM/crash cart and provisioning media present and functional | | |
| Spare drives/PSUs/optics meet OD-POL-02 minimum counts | | |
| All verified items marked "Released for Use" | | |

## 11. KPIs

- Equipment availability at period start ≥ 99.5% of listed items.
- Spares stocking compliance to OD-POL-02 minimums = 100%.
- Availability check completed and signed before period start ≥ 98% of shifts.

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# Phase 2 — Demand intake

# OD-006 — Customer Order / Work Request Intake

**Estimated completion time: 15–45 minutes per request**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

To receive, authenticate, and log all incoming customer orders and service requests — new provisioning, capacity changes, migrations, and support tickets — so that every work item enters the Operations queue with complete, traceable, and correctly classified information.

## 2. Scope

Covers intake and logging of customer orders and work requests across all channels (portal, email, ticketing system, phone) up to the point of queued, ticketed work. Excludes acceptance/capability review — that is, whether the request can be provisioned against available capacity and SLA terms — which is covered under OD-007.

## 3. Responsibilities

- Intake Coordinator (Operations) — receives requests, verifies requester identity and account status, creates and classifies the ticket in the ITSM system.
- Operations Shift Lead — reviews queued intake for completeness and priority, resolves routing questions, approves escalations.
- Service Desk Analyst — captures technical detail on service requests, confirms affected systems/tenants, appends supporting data to the record.

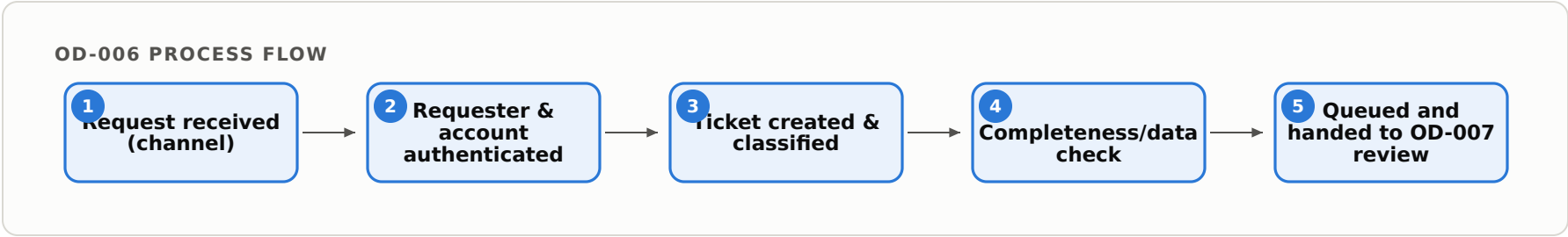
## 4. Required PPE & Lockout/Tagout

- Standard facility PPE (none specific to this task; task is performed at a workstation, not on the data-center floor).
- Not applicable — no hazardous energy involved.

## 5. Regulatory References

- SOC 2 (AICPA Trust Services Criteria) — logical access and processing-integrity controls governing request authentication and record creation.
- ISO/IEC 27001:2022 — information security management for handling customer request data.
- Contractual/regulatory data-handling obligations where applicable (e.g., HIPAA for covered-entity tenants, GDPR/CCPA for personal data in requests). None are universally sector-mandated; where none apply, internal Information Security Policy governs.
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow



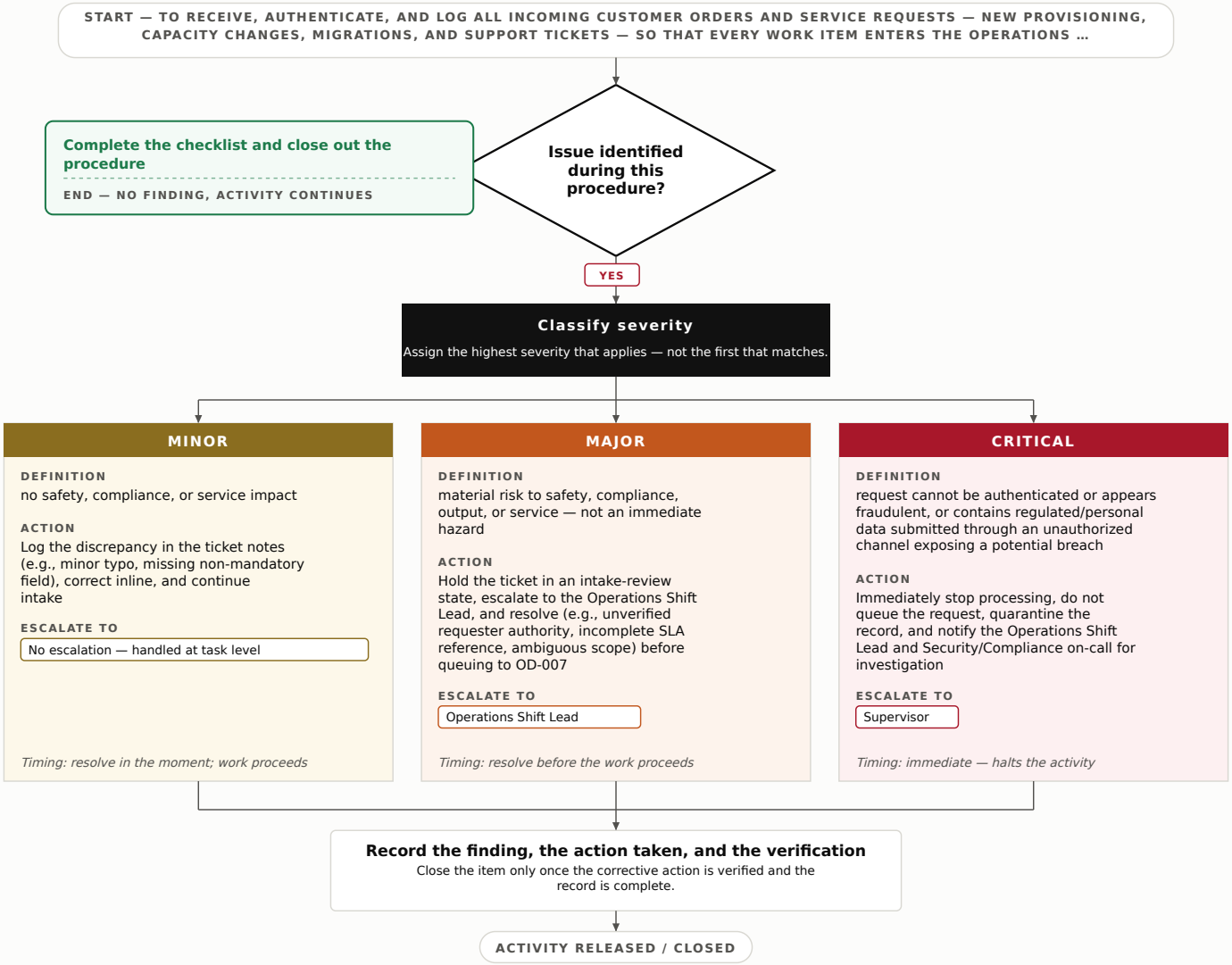

## 7. Step-by-Step Procedure

1. Monitor all intake channels (customer portal, dedicated intake mailbox, ITSM queue, phone) and acknowledge each incoming request within the SLA acknowledgment window.
2. Authenticate the requester against the account record — verify authorized-contact status, account number, and any required security PIN or SSO assertion before proceeding.
3. Determine request type: new provisioning (compute/storage/hosting), capacity or configuration change, data migration, or incident/support request; select the correct ITSM template.
4. Capture required fields — customer/tenant ID, affected systems or services, requested resources, target date, business justification, and applicable SLA/contract reference.
5. Classify priority and impact using the standard priority matrix (severity × affected scope); flag any request touching regulated tenant data.
6. Verify completeness: confirm no mandatory field is blank, contact channel is validated, and any referenced attachments (specs, hardware requests) are legible and attached.
7. Assign the ticket to the correct Operations queue and hand off to OD-007 for acceptance/capability review; notify the requester of the ticket ID and expected next step.
8. Record the intake event, timestamp, classification, and handling notes in the ITSM system; ensure the audit trail is complete and locked.

## 8. Decision Tree

OD-006 · OPERATIONS · DATA HOSTING

## Decision Tree — Customer Order / Work Request Intake




READING THIS TREE

- **No finding** — Activity stands. Complete the checklist and continue.
- **Minor** — Handled in place at task level; no escalation.
- **Major** — Supervisory decision required before the next stage.
- **Critical** — Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- Requester identity and authorized-contact status verified before any ticket is created.
- All mandatory intake fields captured and validated for the selected request type.
- Priority/impact classification matches the standard matrix and regulated-data flag applied where relevant.
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| Request acknowledged within SLA window | | |
| Requester authenticated against account record | | |
| Correct request-type template selected | | |
| All mandatory fields captured and legible | | |
| Priority/impact classification applied correctly | | |
| Regulated-data flag set where applicable | | |
| Ticket handed to OD-007 with complete audit trail | | |

## 11. KPIs

- Acknowledgment within SLA window ≥ 98% of intake requests.
- Intake data completeness (no rework at OD-007) ≥ 95%.
- Authentication failures/fraud escalations logged and actioned 100% within same shift.

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# OD-007 — Order Verification & Acceptance Review

**Estimated completion time: 45–90 minutes per order (excludes large multi-tenant migrations)**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

To confirm that an incoming hosting, colocation, or managed-service order is fully specified, technically deliverable within current capacity, and contractually acceptable before Operations commits resources — preventing over-commitment, SLA breaches, and non-conforming provisioning at this data hosting facility.

## 2. Scope

Covers verification of order scope, technical specification, facility/platform capability, and commercial terms for new and change orders routed to Operations. Excludes order logging (covered under OD-006) and provisioning scheduling (covered under OD-008).

## 3. Responsibilities

- Order Verification Analyst (OD) — reviews order scope, spec, and terms; runs capability check; documents acceptance or rejection.
- Capacity & Infrastructure Lead — confirms compute, storage, power, rack, and bandwidth availability against current utilization.
- Operations Manager — approves acceptance of Major/Critical orders and any terms deviating from the standard service catalog.

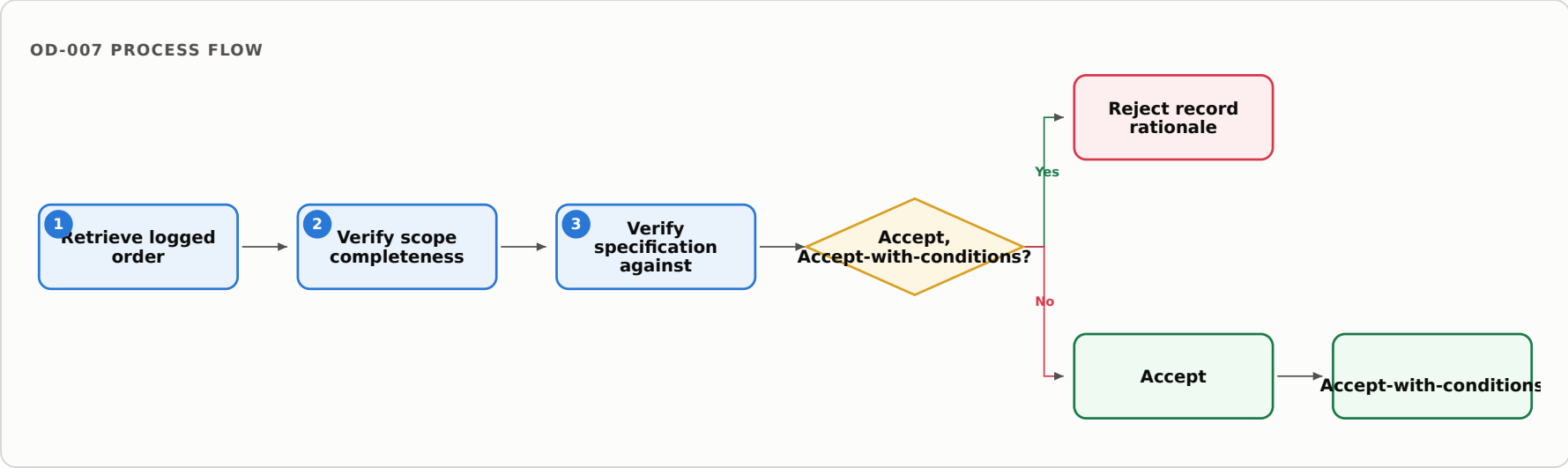
## 4. Required PPE & Lockout/Tagout

- Standard facility PPE; no PPE required for the review itself (desk/console task). ESD wrist strap only if walking the floor to visually confirm rack space.
- Not applicable — no hazardous energy involved in this administrative/verification task.

## 5. Regulatory References

- SOC 2 (AICPA TSC) service commitments; ISO/IEC 27001 Annex A control alignment for provisioning; contractual data-protection terms (e.g., GDPR/HIPAA BAA where the customer's data triggers them); internal Service Acceptance Policy.
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow



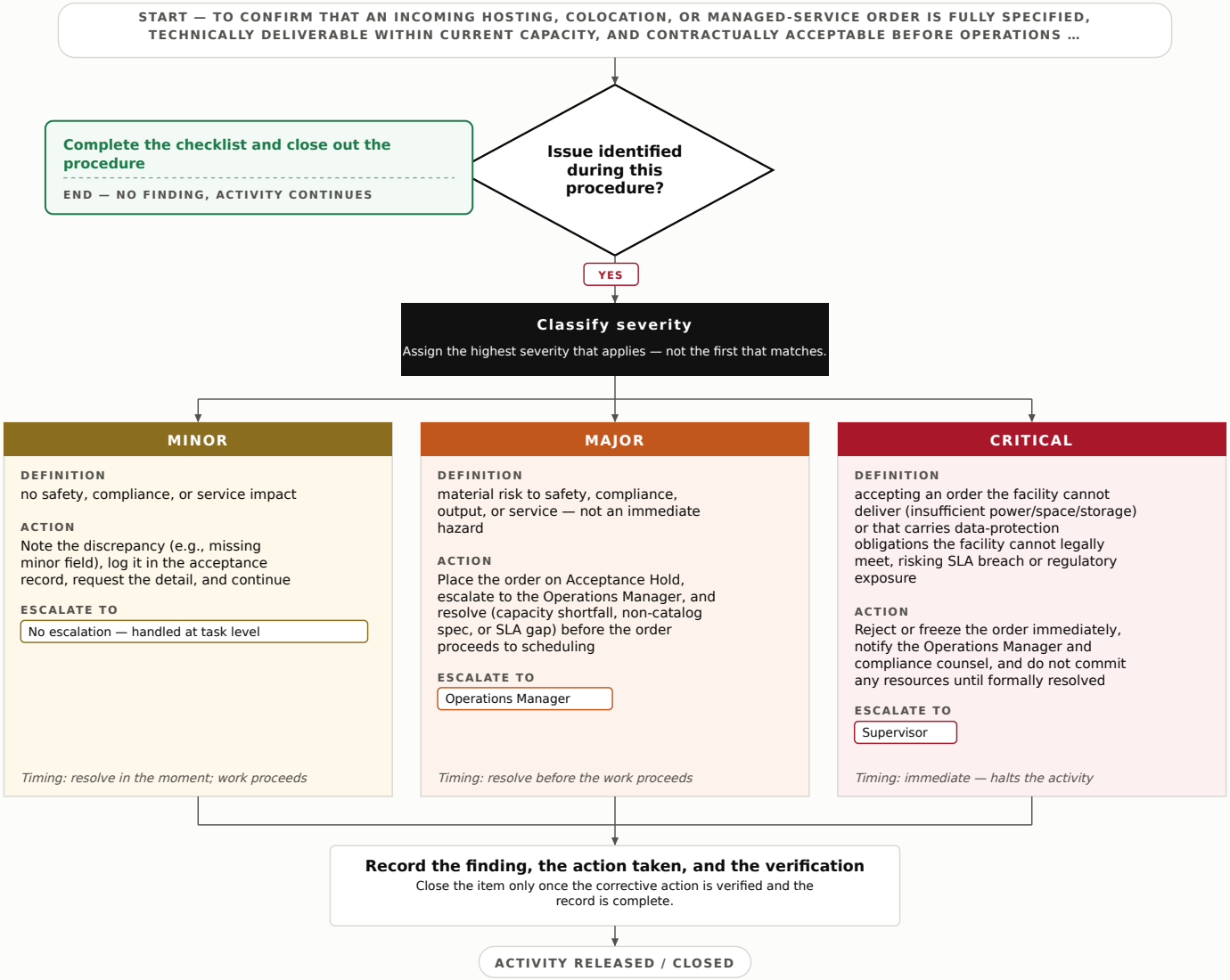

## 7. Step-by-Step Procedure

1. Retrieve the logged order record (per OD-006) and confirm the customer, requested service type (colocation, dedicated compute, cloud/VM, managed backup), and effective date are present.
2. Verify scope completeness: rack units, node count, vCPU/RAM, storage tier and volume, IP/bandwidth allocation, redundancy level, and any migration or onboarding services are explicitly stated.
3. Verify specification against the service catalog — flag any custom configuration, non-standard OS/hypervisor, or hardware not on the approved 334111/334112 build list.
4. Run capability check with the Capacity & Infrastructure Lead: confirm available rack space, power (kW/circuit), cooling headroom, storage array capacity, and network ports meet the requested spec.
5. Review commercial terms: pricing against catalog, contract term length, requested SLA tier, penalty/credit clauses, and any liability caps outside the standard $99 Standard.
6. Review compliance terms: data residency, encryption obligations, BAA/DPA requirements, and audit rights; confirm the facility can meet each without exception.
7. Make the acceptance decision — Accept, Accept-with-conditions, or Reject — and record rationale; hand accepted orders to scheduling (per OD-008).
8. Document the completed verification, sign-off, and any conditions in the order acceptance record.

## 8. Decision Tree

OD-007 · OPERATIONS · DATA HOSTING

## Decision Tree — Order Verification & Acceptance Review




READING THIS TREE

- **No finding** — Activity stands. Complete the checklist and continue.
- **Minor** — Handled in place at task level; no escalation.
- **Major** — Supervisory decision required before the next stage.
- **Critical** — Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- Scope and specification fields fully populated and cross-checked against the service catalog.
- Capacity/capability confirmed in writing by the Capacity & Infrastructure Lead.
- Commercial and compliance terms reconciled against standard acceptable terms; deviations approved.
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| Order scope complete (service type, quantities, effective date) | | |
| Specification matches approved catalog / build list | | |
| Rack, power, cooling, and network capacity confirmed available | | |
| Storage tier and volume available on target array | | |
| SLA tier and pricing within standard terms (deviations approved) | | |
| Data-protection / residency obligations deliverable | | |
| Acceptance decision recorded with rationale and sign-off | | |

## 11. KPIs

- Orders verified within target turnaround (≤ 1 business day): ≥ 95%
- Accepted orders later found non-deliverable (post-acceptance capacity/spec failure): ≤ 1%
- Acceptance records complete with sign-off and rationale: 100%

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# OD-008 — Job Scheduling & Sequencing

**Estimated completion time: 30–60 minutes per scheduling cycle (daily); 10–15 minutes for ad-hoc insertion**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

To place accepted hosting and data-processing work — provisioning requests, batch jobs, migrations, backup and restore runs, and scheduled reports — into the operating schedule so that each job is sequenced by contractual priority and due date, avoiding SLA breaches and capacity collisions.

## 2. Scope

Covers the ordering and calendar placement of accepted work items across the production schedule and change-window calendar for the data center's compute, storage, and network resources. Excludes assignment of specific staff or hardware to a scheduled job, which is covered under OD-009; excludes planned maintenance-window scheduling, which is covered under PM-008.

## 3. Responsibilities

- Operations Scheduler — builds and maintains the operating schedule, sequences jobs by priority and due date, and confirms no window collisions.
- Shift Operations Lead — reviews and approves the daily schedule, arbitrates priority conflicts, and authorizes ad-hoc insertions.
- Service Delivery Coordinator — validates customer SLA tiers and due-date commitments against accepted work before it is scheduled.

## 4. Required PPE & Lockout/Tagout

- Standard facility PPE for NOC/data-floor access (badge, ESD precautions if entering equipment rows); scheduling itself is performed from the operations console.
- Not applicable — no hazardous energy involved; this is an administrative coordination task.

## 5. Regulatory References

- None sector-specific mandating job sequencing; internal Operations Scheduling Policy and customer Master Service Agreements / SLA schedules govern. Supporting frameworks: SOC 2 (AICPA TSC) availability/processing-integrity criteria and ISO/IEC 27001 A.12 operational procedures where the facility is certified.
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow

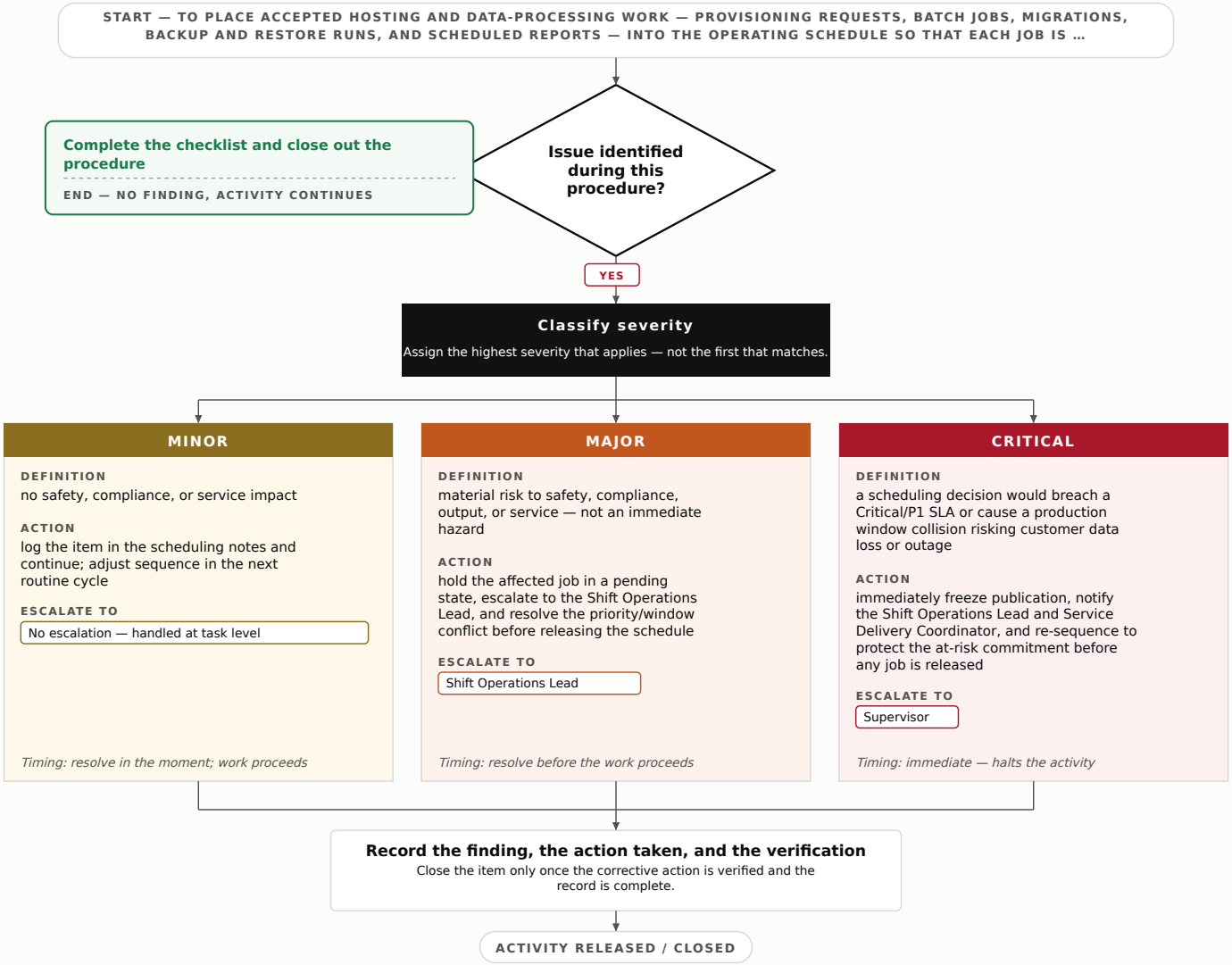

## 7. Step-by-Step Procedure

1. Pull all accepted work items from the intake queue (provisioning tickets, batch jobs, migration and restore requests) that are ready for scheduling.
2. Confirm each item's SLA tier and due-date commitment with the Service Delivery Coordinator; flag any item missing a validated priority.
3. Rank items by priority tier first (Critical/P1 → routine/P4), then by due date within each tier, applying documented tie-break rules for equal-priority items.
4. Map each ranked item onto the operating schedule against available production and change windows, reserving buffer for known blackout periods (do not schedule into a maintenance window owned by PM-008).
5. Run a collision and capacity check to confirm no two jobs contend for the same resource window and that cumulative load fits available capacity headroom.
6. Reconcile any conflicts with the Shift Operations Lead; reorder or defer lower-priority items and record the rationale for each deferral.
7. Publish the finalized operating schedule to the NOC and hand off resource-assignment detail to OD-009.
8. Record the completed schedule, priority decisions, and any deferrals in the scheduling log with timestamp and approver.

## 8. Decision Tree

OD-008 · OPERATIONS · DATA HOSTING

## Decision Tree — Job Scheduling & Sequencing




READING THIS TREE

- **No finding** — Activity stands. Complete the checklist and continue.
- **Minor** — Handled in place at task level; no escalation.
- **Major** — Supervisory decision required before the next stage.
- **Critical** — Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- Every scheduled item carries a validated SLA tier and due date before placement.
- No two jobs share a contended resource window in the published schedule.
- All deferrals and priority overrides are logged with rationale and approver.
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| All accepted work items pulled from intake queue | | |
| SLA tier and due date validated for each item | | |
| Items ranked by priority then due date | | |
| No window collisions or capacity overloads | | |
| Deferrals recorded with rationale | | |
| Schedule published to NOC and handed to OD-009 | | |
| Scheduling log timestamped and approved | | |

## 11. KPIs

- SLA-driven jobs scheduled within due-date commitment: ≥ 99%
- Window collisions in published schedule: 0 per cycle
- Ad-hoc insertions requiring re-sequencing of published schedule: ≤ 5% of scheduled jobs

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# OD-009 — Resource & Capacity Allocation

**Estimated completion time: 45–90 minutes per allocation cycle (per shift or per work order)**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

Assign qualified technicians, server/storage hardware, and cabinet/floor space to scheduled data center work so that committed capacity is physically real — power, cooling, rack units, and licensed personnel — before work is dispatched. This prevents overcommitment of the raised-floor and power/cooling envelope common to Data Processing and Hosting operations.

## 2. Scope

Covers allocation and confirmation of people, equipment (servers, storage arrays, PDUs, network gear), and physical space (rack units, cabinet positions, floor tiles) against already-scheduled work orders. Excludes staffing presence and shift coverage (see OD-003) and schedule sequencing/ordering of work (see OD-008); this procedure only confirms that resources named in an existing schedule are real and available.

## 3. Responsibilities

- Operations Shift Lead — owns the allocation cycle; assigns technicians and hardware to work orders and confirms real capacity before release.
- Facilities Engineer — verifies power (kW/circuit), cooling headroom, and floor-loading limits for each proposed placement.
- Capacity/Provisioning Coordinator — maintains the DCIM rack/space inventory and reconciles committed vs. available capacity.

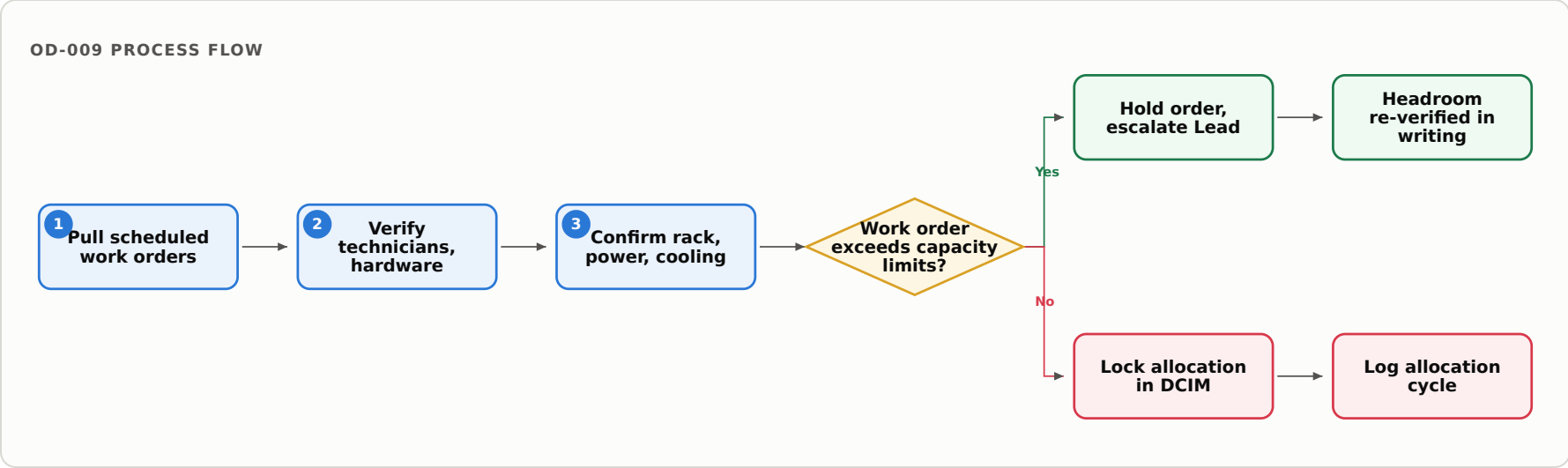
## 4. Required PPE & Lockout/Tagout

- Standard facility PPE: ESD wrist strap and heel grounding when handling live hardware; closed-toe footwear on the raised floor.
- Lockout/Tagout: Applicable only where allocation requires energizing/de-energizing a PDU or branch circuit — follow facility LOTO before touching electrical distribution; otherwise Not applicable to the allocation task itself.

## 5. Regulatory References

- ANSI/TIA-942 (Telecommunications Infrastructure Standard for Data Centers) — space, power, and redundancy classification.
- NFPA 70 (NEC) Article 645 — Information Technology Equipment rooms; branch-circuit and power capacity limits.
- NFPA 75 — fire protection of information technology equipment; equipment spacing/loading.
- OSHA 29 CFR 1910.303 / 1910.147 — electrical installation and hazardous-energy control where PDUs/circuits are involved.
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow



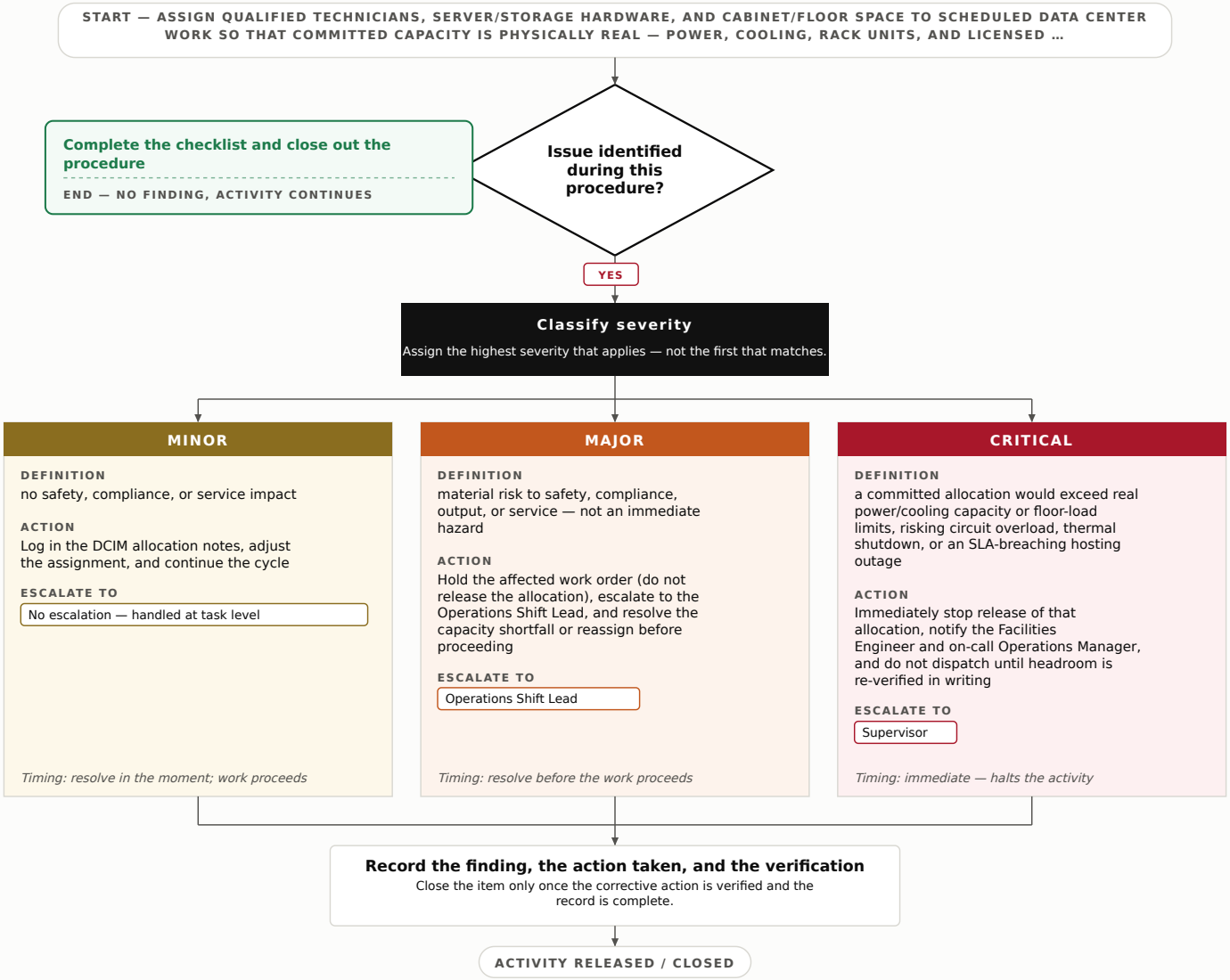

## 7. Step-by-Step Procedure

1. Pull the current set of scheduled work orders from the DCIM/ticketing system that require resource assignment this cycle (do not re-sequence — sequence is fixed per OD-008).
2. For each work order, identify required technician skills/certifications and confirm a qualified technician is assignable (availability itself is confirmed per OD-003).
3. Verify required hardware is physically on hand — servers (334111), storage devices (334112), PDUs and electrical gear (335999) — and confirm serial/asset tags against the intended work order in DCIM.
4. Verify target rack space: confirm free rack units, cabinet weight/floor-loading limit, and cable-pathway availability at the intended position.
5. Confirm power headroom with the Facilities Engineer — available amps/kW on the target branch circuit and PDU, including N+1 redundancy margin — and confirm cooling headroom for the added thermal load.
6. Reconcile total committed capacity against available capacity; flag any work order that would exceed power, cooling, space, or skilled-labor limits.
7. Commit confirmed allocations by locking the assignment in DCIM and updating the reserved-capacity ledger.
8. Document the allocation cycle: record assignments, confirmed headroom figures, any flags, and dispositions in the DCIM allocation log.

## 8. Decision Tree

OD-009 · OPERATIONS · DATA HOSTING

## Decision Tree — Resource & Capacity Allocation




READING THIS TREE

- **No finding** — Activity stands. Complete the checklist and continue.
- **Minor** — Handled in place at task level; no escalation.
- **Major** — Supervisory decision required before the next stage.
- **Critical** — Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- Every committed work order has a named qualified technician and a confirmed hardware asset tag.
- Power and cooling headroom confirmed by Facilities Engineer for each placement, including redundancy margin.
- Reserved-capacity ledger in DCIM reconciles to zero over-commitment.
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| Each scheduled work order has a qualified technician assigned | | |
| Required hardware physically on hand and asset-tagged in DCIM | | |
| Target rack units available and cabinet weight/floor-load within limit | | |
| Branch-circuit / PDU power headroom confirmed (incl. N+1 margin) | | |
| Cooling headroom confirmed for added thermal load | | |
| Reserved-capacity ledger reconciled — no over-commitment | | |
| Allocation cycle documented in DCIM log | | |

## 11. KPIs

- Allocation accuracy (committed resources found real at dispatch): ≥ 99%
- Power/cooling over-commitment incidents: 0 per quarter
- Allocation cycle completed before scheduled dispatch window: 100%

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# OD-010 — Incoming Material / Supply Verification

**Estimated completion time: 30–60 minutes per inbound delivery**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

To confirm that inbound hardware and supplies — rack servers, storage devices, power/electrical components, and spares — arriving at the data hosting facility match the purchase order in identity, quantity, and condition before they enter the asset management and staging workflow. This protects capacity commitments, warranty coverage, and chain-of-custody for customer-serving infrastructure.

## 2. Scope

Covers verification of inbound materials/supplies against the purchase order, line-item quantities, and outward physical condition at the point of intake by Operations. Excludes spec-conformance testing (burn-in / firmware / functional validation), which is covered under QC-003; excludes putaway to rack or storage location, covered under WH-006; and excludes the receiving-dock count, covered under SH-008.

## 3. Responsibilities

- Receiving Operations Technician — performs the PO-to-shipment match, records serial/asset tags, and inspects condition of each line item.
- Facilities Operations Lead — resolves discrepancies, authorizes acceptance or quarantine, and approves supplier follow-up.
- Hardware Asset Coordinator — enters verified units into the asset/CMDB register and confirms warranty and RMA data capture.

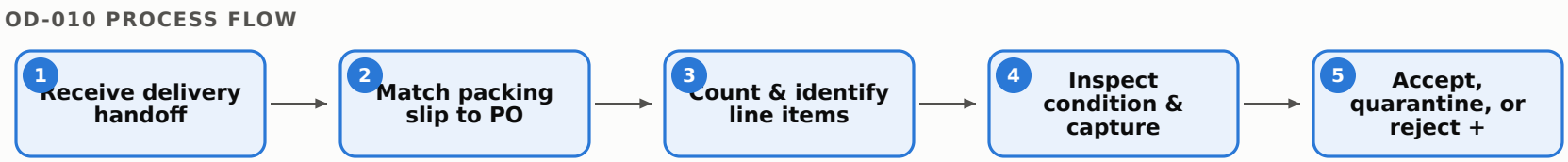
## 4. Required PPE & Lockout/Tagout

- Standard facility PPE: ESD wrist strap/heel grounding when handling exposed circuit boards or storage media; cut-resistant gloves for uncrating; safety footwear in the intake/staging area.
- Not applicable — no hazardous energy involved; equipment is unpowered and remains de-energized during verification.

## 5. Regulatory References

- None sector-specific to receiving verification; internal Asset Intake & Chain-of-Custody Policy applies. Related frameworks that govern downstream handling of this hardware: SOC 2 (Trust Services Criteria, physical/asset controls) and ISO/IEC 27001 Annex A (A.7 asset management, A.8 media handling) as adopted by the facility; RoHS/WEEE documentation retained where supplied.
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow



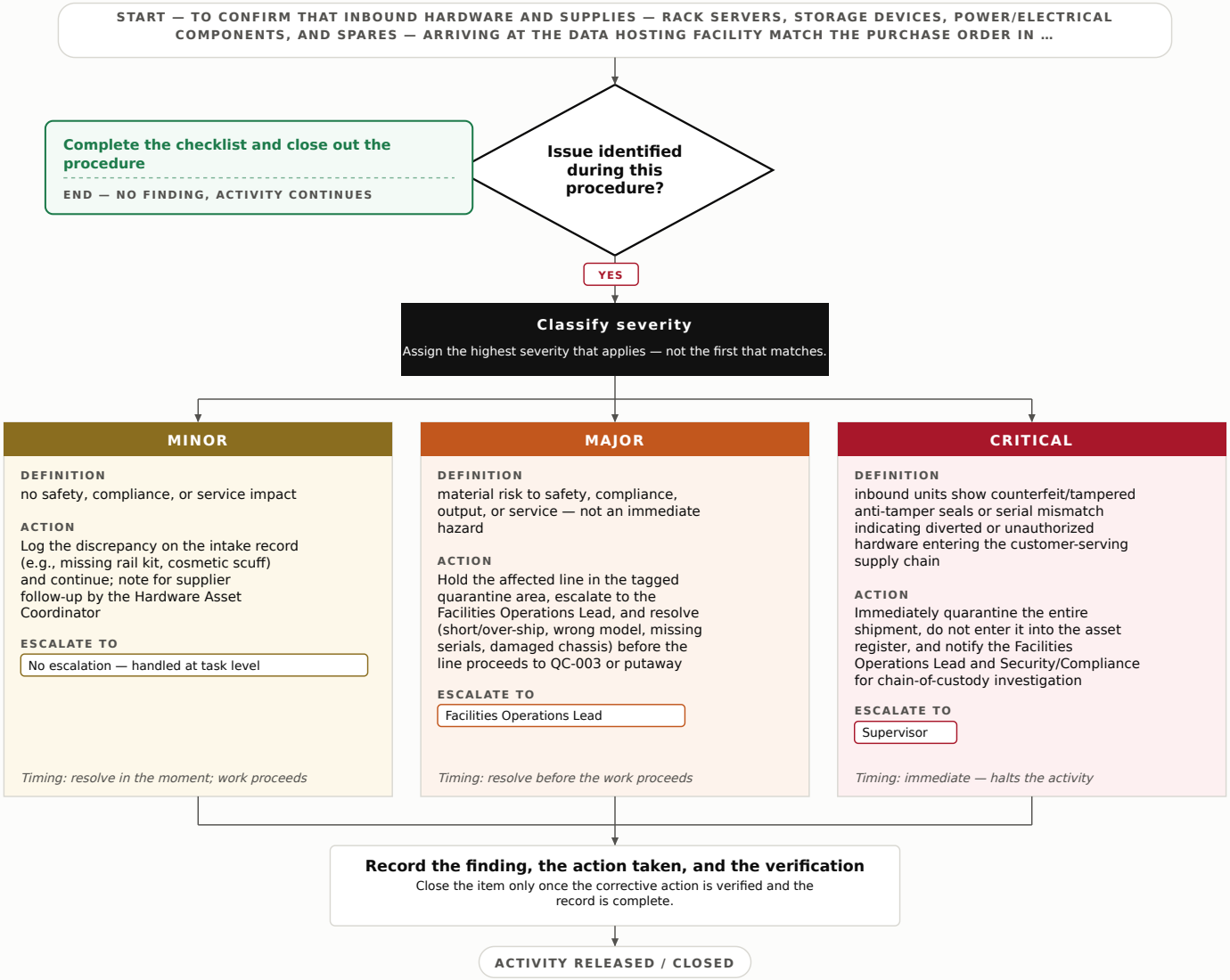

## 7. Step-by-Step Procedure

1. Retrieve the open purchase order and expected-delivery record for the inbound shipment; confirm supplier and PO number against the packing slip.
2. Verify each line item on the packing slip corresponds to an ordered SKU/part (server models, storage drives, PSUs, PDUs, rail kits, spares); flag any unlisted or substituted items.
3. Confirm delivered quantity per line matches the PO quantity; accept the SH-008 dock count as the controlling piece count and reconcile line-level quantities against it.
4. Inspect each unit's outward condition: crushed/punctured packaging, shock/tilt indicators, moisture, bent chassis, damaged connectors, or ESD-bag breach.
5. Record manufacturer serial numbers and asset tags for each server, storage device, and electrical component; photograph any damage before further handling.
6. Verify warranty/entitlement paperwork, RoHS/WEEE and RMA references, and country-of-origin documentation are present for each qualifying line.
7. Classify each line as Accept, Quarantine, or Reject per Section 8; place quarantined/rejected units in the tagged hold area and do NOT release to QC-003 or putaway.
8. Complete the Inspection Checklist, enter verified units into the asset/CMDB register, and route accepted lines to QC-003 for spec-conformance testing.

## 8. Decision Tree

OD-010 · OPERATIONS · DATA HOSTING

## Decision Tree — Incoming Material / Supply Verification




READING THIS TREE

- **No finding** — Activity stands. Complete the checklist and continue.
- **Minor** — Handled in place at task level; no escalation.
- **Major** — Supervisory decision required before the next stage.
- **Critical** — Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- 100% of PO line items reconciled against packing slip and SH-008 dock count.
- Serial/asset tags captured and legible for every accepted server, storage device, and electrical component.
- All damage documented with photos and warranty/RMA paperwork retained.
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| Packing slip matches PO number and supplier | | |
| Line-item SKUs/part numbers match ordered items | | |
| Delivered quantities reconcile to dock count (SH-008) | | |
| Packaging & shock/tilt indicators intact | | |
| No visible chassis/connector/media damage | | |
| Serial numbers & asset tags recorded | | |
| Warranty / RoHS-WEEE / RMA documentation present | | |

## 11. KPIs

- PO-to-shipment match accuracy ≥ 99%
- Serial/asset capture completeness = 100% of accepted units
- Verification cycle time per delivery ≤ 60 minutes

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# Phase 3 — Execution

# OD-011 — Standard Work Execution & Process Adherence

**Estimated completion time: 30–60 minutes per shift cycle (per method-controlled runbook execution)**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

This procedure ensures that recurring data hosting operations tasks — provisioning, patching, backup verification, environmental monitoring rounds, and ticket-driven changes — are executed to the documented standard method (runbook) so outcomes are consistent, auditable, and SLA-compliant, and so any departure from method is caught and logged.

## 2. Scope

Covers execution of approved operations runbooks in the production and staging data center environments and the identification and logging of deviations from the defined method. Excludes in-process quality checks, which are covered under QC-007, and safe-work method, which is covered under SD-005.

## 3. Responsibilities

- Data Center Operations Technician — executes the runbook step-by-step, records completion, flags any deviation from the defined method.
- Operations Shift Lead — confirms the correct runbook version is in use, authorizes change windows, receives and dispositions escalations.
- Operations Manager — owns runbook standards, reviews Critical deviations, approves method changes and corrective actions.

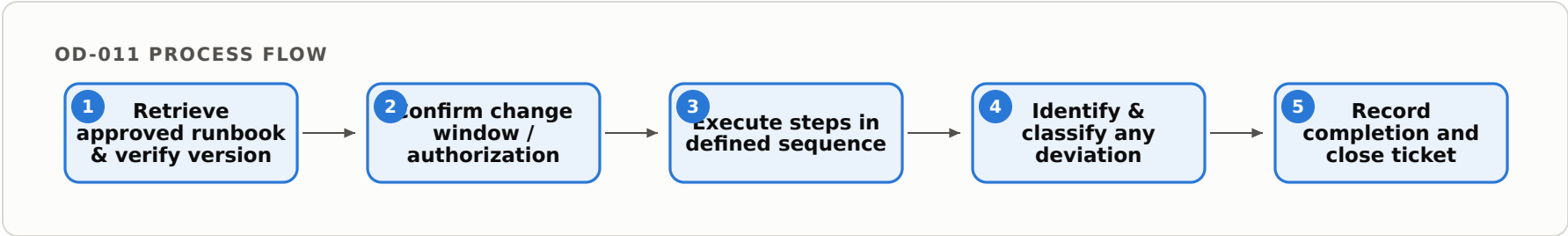
## 4. Required PPE & Lockout/Tagout

- Standard facility PPE for data hall entry: ESD wrist strap when handling hardware, hearing awareness in hot/cold aisles, badge-controlled access.
- Lockout/Tagout: Not applicable for standard execution — no hazardous energy work under this procedure; energized-hardware isolation is governed under SD-005.

## 5. Regulatory References

- SOC 2 (AICPA Trust Services Criteria) common-control change management and operations requirements
- ISO/IEC 27001:2022 Annex A operational and change-control controls
- None additional sector-specific; internal Operations Runbook Standard and Change Management Policy apply.
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow



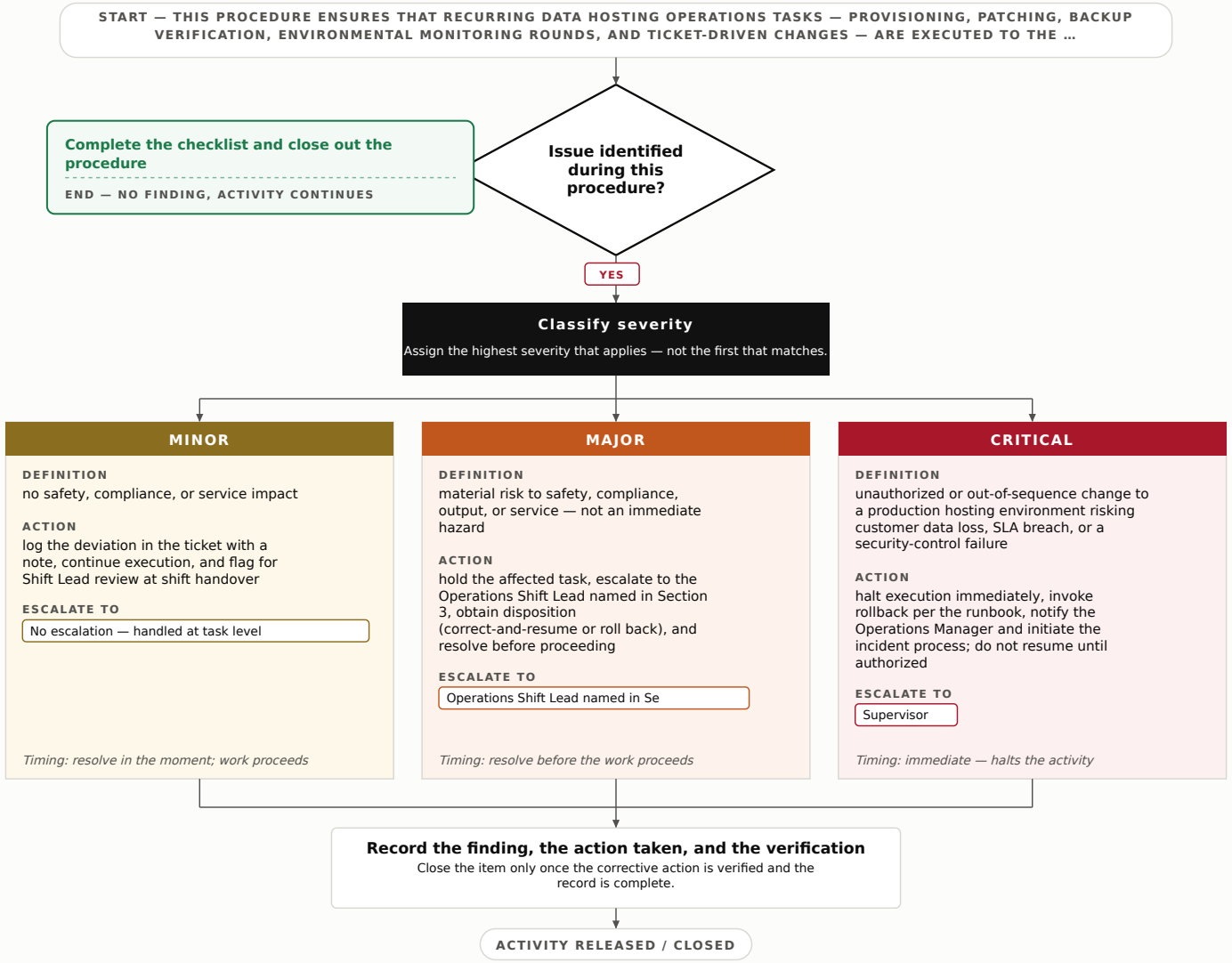

## 7. Step-by-Step Procedure

1. Open the assigned work ticket and retrieve the current approved runbook; confirm the version matches the Operations Runbook Standard register.
2. Verify authorization: confirm the change window is open and the Shift Lead has approved the task for this environment (production vs. staging).
3. Stage prerequisites named in the runbook (credentials, tooling access, target host/rack identifiers, rollback plan reference).
4. Execute each runbook step in the defined order; do not skip, reorder, or substitute steps without documented Shift Lead approval.
5. Record actual values and timestamps at each checkpoint step (e.g., host provisioned, patch applied, backup job confirmed complete).
6. Where actual execution differs from the defined method, stop, note the deviation, and classify it per the Decision Tree (Section 8).
7. On completion, confirm the outcome matches the runbook expected end-state and update the ticket status.
8. Document execution: attach the completed runbook record, deviation log entries, and timestamps to the ticket and close out per records policy.

## 8. Decision Tree

OD-011 · OPERATIONS · DATA HOSTING

## Decision Tree — Standard Work Execution & Process Adherence




READING THIS TREE

- **No finding** — Activity stands. Complete the checklist and continue.
- **Minor** — Handled in place at task level; no escalation.
- **Major** — Supervisory decision required before the next stage.
- **Critical** — Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- Correct runbook version confirmed against register before start
- Change-window authorization verified for the target environment
- All steps executed in defined sequence with recorded timestamps
- Zero unresolved Critical findings

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| Approved runbook version matches register | | |
| Change window open and authorized | | |
| Prerequisites staged per runbook | | |
| Steps executed in defined sequence | | |
| Actual values/timestamps recorded at checkpoints | | |
| Deviations logged and classified | | |
| End-state matches runbook expectation; ticket closed | | |

## 11. KPIs

- Runbook adherence rate (steps executed as defined) ≥ 98%
- Unauthorized/out-of-sequence change rate ≤ 1% of executions
- Deviation logging completeness (deviations logged vs. detected) = 100%

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# OD-012 — Work-in-Progress Tracking & Status Update

**Estimated completion time: 15–30 minutes per shift-cycle update; ad hoc on status change**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

To ensure the current status of every active job in the Operations queue — provisioning tickets, migration runs, hardware installs, and scheduled maintenance windows — is accurately recorded and visible to Operations staff and dependent teams so hand-offs and customer commitments are met without gaps.

## 2. Scope

Covers status capture, state transitions, and visibility of active Operations work-in-progress in the ticketing/ITSM and change-management systems. Excludes throughput/volume measurement, which is covered under OD-014, and quality/defect data capture, which is covered under QC-027.

## 3. Responsibilities

- Operations Shift Lead — owns the WIP board, verifies each active job carries a current, accurate state at shift open and close, and drives escalations.
- Data Center Technician — updates ticket status in real time as provisioning, install, or maintenance steps complete or stall.
- NOC Coordinator — reconciles the WIP board against monitoring alerts and customer-facing status commitments; flags stale or blocked items.

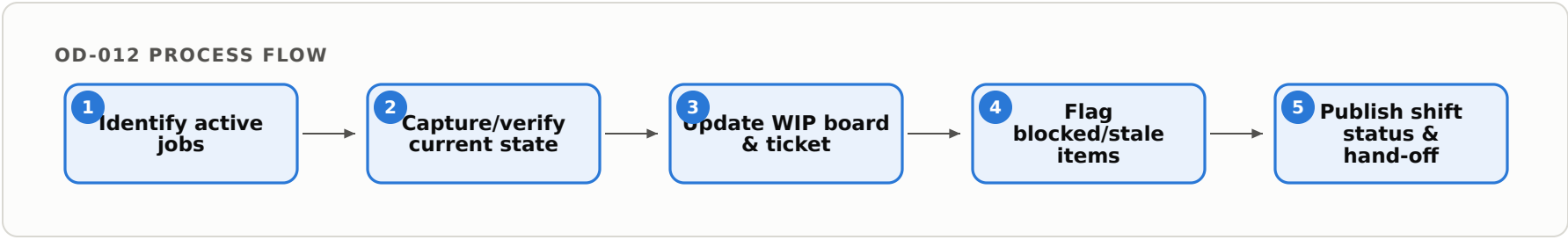
## 4. Required PPE & Lockout/Tagout

- Standard facility PPE when on the data hall floor (ESD wrist strap for rack work); none required for console-based status updates.
- Not applicable — no hazardous energy is controlled by this administrative task; any physical rack/PDU work is governed by its own maintenance LOTO procedure.

## 5. Regulatory References

- None sector-specific to status tracking; internal Operations WIP-tracking policy and customer SLA/contract terms apply. Where in-scope customer data governs, SOC 2 (AICPA TSC) change-management and availability criteria and ISO/IEC 27001 A.12/A.14 change-control controls inform record-keeping practice.
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow



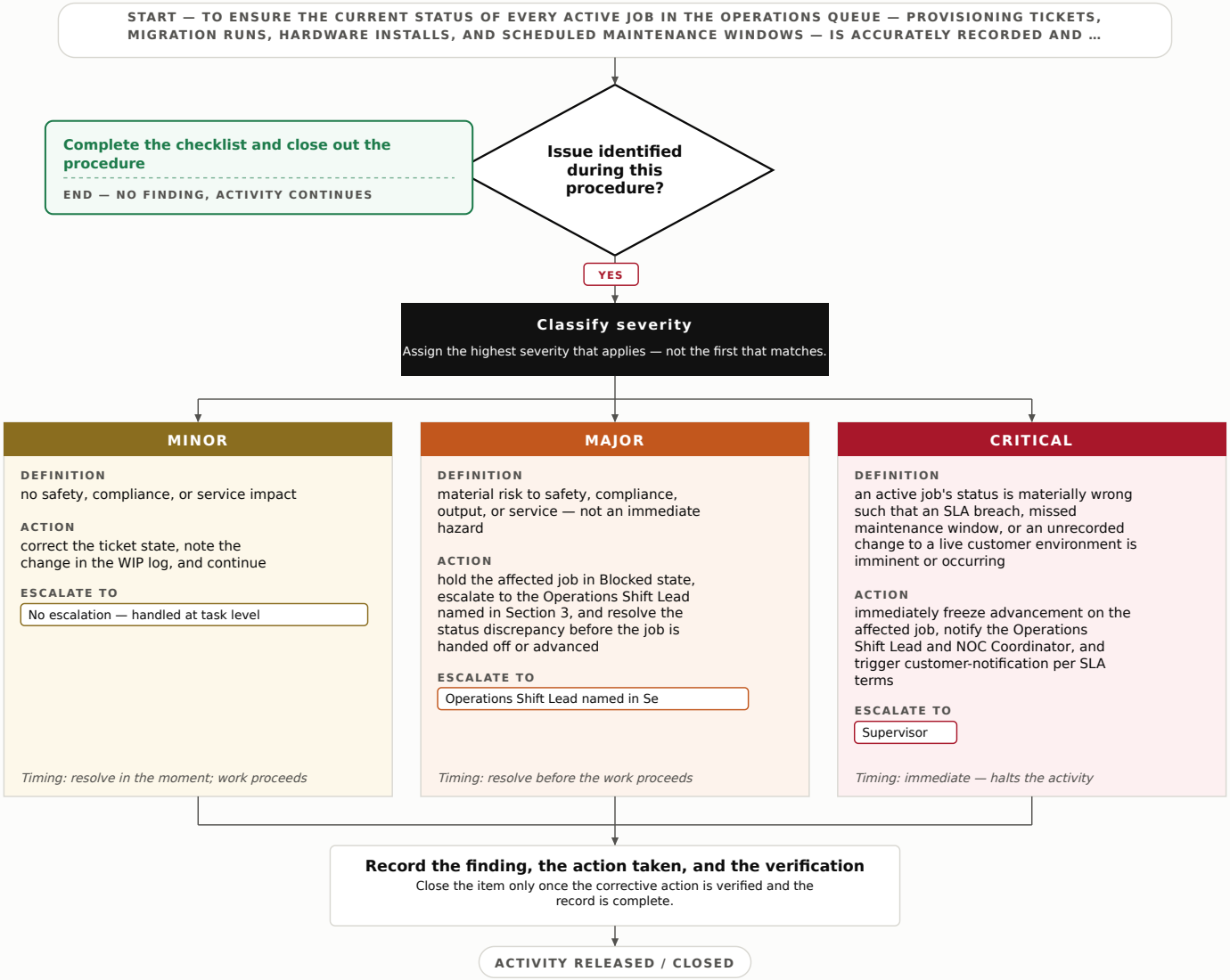

## 7. Step-by-Step Procedure

1. At shift open, pull the list of all open Operations jobs (provisioning, migration, install, maintenance windows) from the ITSM queue and the change calendar.
2. For each job, confirm the recorded state matches reality — verify with the assigned Technician or monitoring evidence, not assumption.
3. Set each job to its correct WIP state: Queued, In Progress, Blocked, Awaiting Customer, or Ready for Hand-off.
4. For any Blocked or Awaiting Customer item, record the blocker, owner, and expected clear date in the ticket notes.
5. Identify stale items (no state change past their SLA checkpoint) and route them to the NOC Coordinator for reconciliation against customer commitments.
6. Confirm the WIP board reflects all changes and is visible on the Operations dashboard for dependent teams.
7. At shift close, perform hand-off: walk the incoming Shift Lead through active, blocked, and at-risk jobs and confirm acknowledgement.
8. Record the update timestamp, updater, and any escalations in the WIP log for the shift record.

## 8. Decision Tree

OD-012 · OPERATIONS · DATA HOSTING

## Decision Tree — Work-in-Progress Tracking & Status Update




READING THIS TREE

- **No finding** — Activity stands. Complete the checklist and continue.
- **Minor** — Handled in place at task level; no escalation.
- **Major** — Supervisory decision required before the next stage.
- **Critical** — Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- Every open Operations job carries a current WIP state at shift open and close.
- All Blocked/Awaiting Customer items have a recorded blocker, owner, and expected clear date.
- Shift hand-off acknowledged by incoming Shift Lead and logged.
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| All active jobs present on WIP board (none orphaned in queue) | | |
| Recorded state matches verified reality for each job | | |
| Blocked/Awaiting items have owner + expected clear date | | |
| Stale items flagged and routed to NOC Coordinator | | |
| WIP dashboard visible to dependent teams | | |
| Shift hand-off acknowledged and logged | | |
| Update timestamp and updater recorded in WIP log | | |

## 11. KPIs

- WIP board accuracy (states matching verified reality) ≥ 98% at each audit.
- Stale-item rate (jobs past SLA checkpoint without update) ≤ 2% at shift close.
- Hand-off completeness (shifts with acknowledged, fully logged hand-off) 100%.

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# OD-013 — Operational Handoff Between Work Stages

**Estimated completion time: 15–45 minutes per handoff event**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

This procedure defines the controlled transfer of active operational work — provisioning jobs, migration runbooks, incident tickets, and change windows — between processing stages, crews, or NOC/DC-Ops functions so that no in-flight task at the data hosting facility is dropped, duplicated, or advanced without a verified owner and complete context.

## 2. Scope

Covers the structured handoff of live work items between operational stages, crews, or functional teams within Operations, including transfer of ticket ownership, runbook position, access state, and outstanding actions. Excludes end-of-shift personnel changeover, which is covered under OD-002, and stage quality release/sign-off, which is covered under QC-013.

## 3. Responsibilities

- Shift Operations Lead (NOC) — owns the handoff event, confirms receiving owner acceptance, and authorizes work to advance to the next stage.
- Outgoing Stage Operator — assembles the handoff package (ticket state, runbook step, open actions, access notes) and remains available until acceptance is confirmed.
- Incoming Stage Operator — reviews the package, acknowledges ownership in the ticketing/ITSM system, and raises any gaps before accepting.

## 4. Required PPE & Lockout/Tagout

- Standard facility PPE for any handoff conducted on the data hall floor (ESD wrist strap when touching mounted hardware; hearing awareness in cold-aisle zones).
- Not applicable — no hazardous energy control performed during this procedure; physical LOTO on power/cooling systems is out of scope.

## 5. Regulatory References

- SOC 2 Trust Services Criteria (AICPA) — CC7/CC8 change and operations controls; ISO/IEC 27001:2022 A.5.23 / A.8.32 (change management and operational handoff of information processing); internal Operations Runbook Control Policy (OD-POL-004).
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow

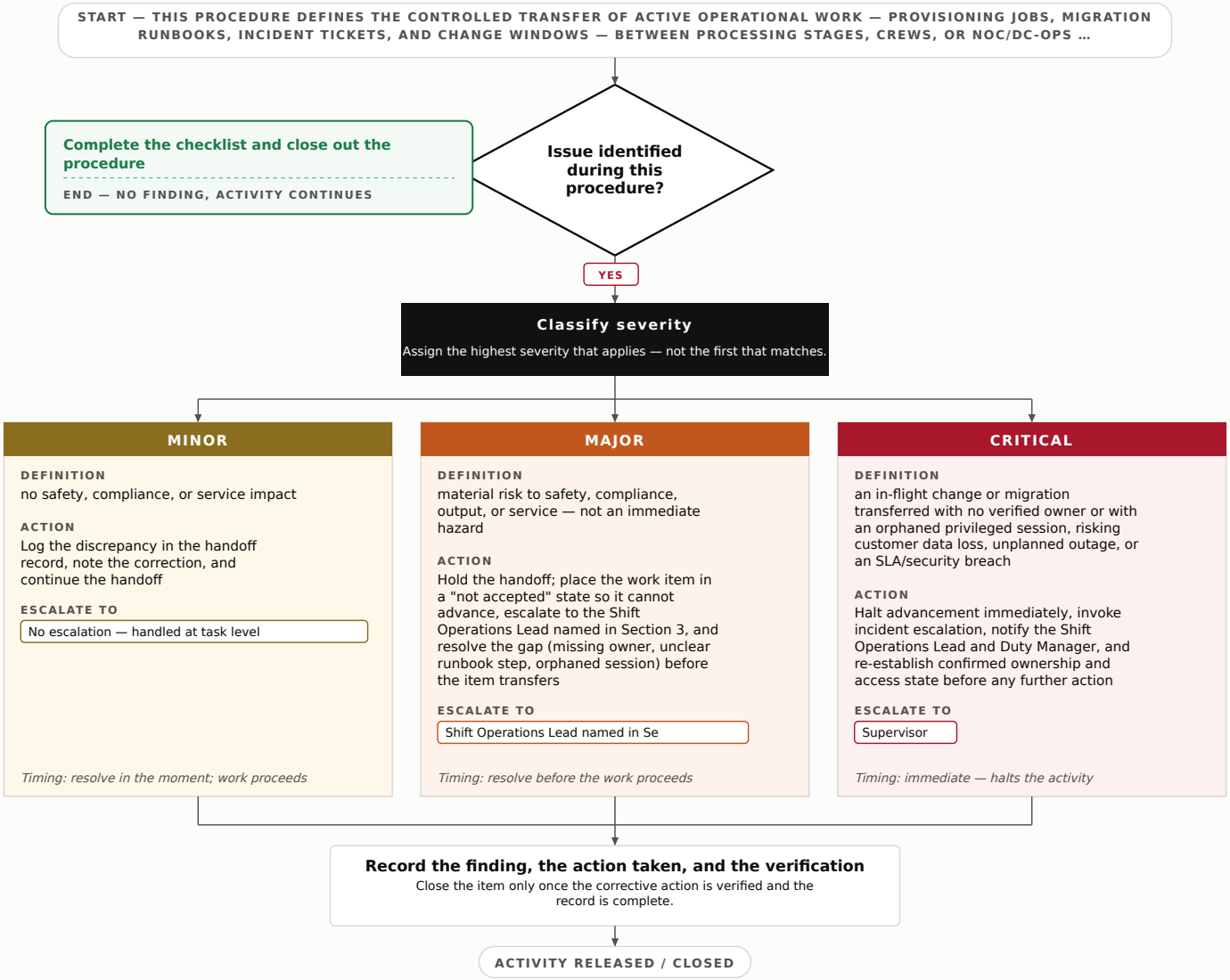

## 7. Step-by-Step Procedure

1. Identify the handoff trigger — completion of a stage milestone, crew rotation within a job, or transfer of a live ticket/change window between functional teams.
2. Outgoing operator freezes the work item at a defined checkpoint: record current runbook step, ticket state, affected assets (rack/host/storage IDs), and any active change-window timers.
3. Assemble the handoff package: open actions, dependencies, customer/SLA context, escalation contacts, and current access/session state (privileged sessions closed or explicitly transferred, never left orphaned).
4. Notify the Incoming Stage Operator and Shift Operations Lead through the ITSM tool; do not proceed on verbal-only handoff.
5. Incoming operator reviews the package against the live system state — confirms runbook position, verifies asset IDs match, and validates that no dependent job is mid-flight without an owner.
6. Incoming operator raises any gaps for resolution; once clear, formally accepts ownership by reassigning the ticket and time-stamping acceptance.
7. Shift Operations Lead confirms acceptance and authorizes the work to advance to the next stage or crew.
8. Log the completed handoff (item, from/to owner, timestamp, package reference) in the ITSM handoff record and close out the procedure.

## 8. Decision Tree

OD-013 · OPERATIONS · DATA HOSTING

## Decision Tree — Operational Handoff Between Work Stages




READING THIS TREE

- **No finding** — Activity stands. Complete the checklist and continue.
- **Minor** — Handled in place at task level; no escalation.
- **Major** — Supervisory decision required before the next stage.
- **Critical** — Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- Every handoff has a single, named, ITSM-recorded incoming owner before work advances.
- Runbook position and affected asset IDs verified against live system state at acceptance.
- All privileged sessions closed or explicitly transferred — no orphaned access at boundary.
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| Handoff package complete (state, step, open actions, assets) | | |
| Incoming owner acknowledged ownership in ITSM | | |
| Runbook step and asset IDs match live state | | |
| No orphaned privileged sessions at boundary | | |
| Active change-window timers/SLA context transferred | | |
| Shift Operations Lead authorization recorded | | |
| Handoff logged with timestamp and package reference | | |

## 11. KPIs

- Handoffs with verified single owner at acceptance: 100%
- Dropped/duplicated work items attributable to handoff: 0 per quarter
- Median handoff acceptance time from package delivery: ≤ 15 minutes

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# OD-014 — Output Monitoring & Throughput Review

**Estimated completion time: 30–60 minutes per monitoring interval (per shift or per defined review window)**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

This procedure defines how Operations personnel monitor the rate and volume of operational output — ingest throughput, processing job completion, provisioning fulfillment, and platform request-handling — against the capacity plan for the hosting environment, so deviations are detected and routed before they degrade service or breach SLA commitments.

## 2. Scope

Covers interval-based observation of output rate/volume against planned targets across the hosting fleet, including data-ingest pipelines, batch/stream processing queues, and customer-facing platform request rates. Excludes KPI definition and formal KPI review, which is covered under OD-028, and process-capability analysis, which is covered under QC-026.

## 3. Responsibilities

- Operations Analyst — pulls throughput and volume metrics at each review interval, compares actuals to plan, and records findings.
- Shift Operations Lead — reviews flagged deviations, classifies severity, and authorizes containment or escalation.
- Operations Manager — owns capacity-plan baselines, receives Major/Critical escalations, and approves plan or resourcing adjustments.

## 4. Required PPE & Lockout/Tagout

- Standard facility PPE for any observation performed inside the data-hall (hearing awareness, closed-toe footwear); none required for remote/NOC-based monitoring.
- Not applicable — no hazardous energy involved; this is a monitoring and review task performed against telemetry dashboards and logs.

## 5. Regulatory References

- None sector-specific to output monitoring; internal Operations capacity-management policy and customer SLA agreements apply. Where customer data governs, SOC 2 (AICPA TSC — Availability & Processing Integrity) and applicable contractual availability commitments inform review thresholds.
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow

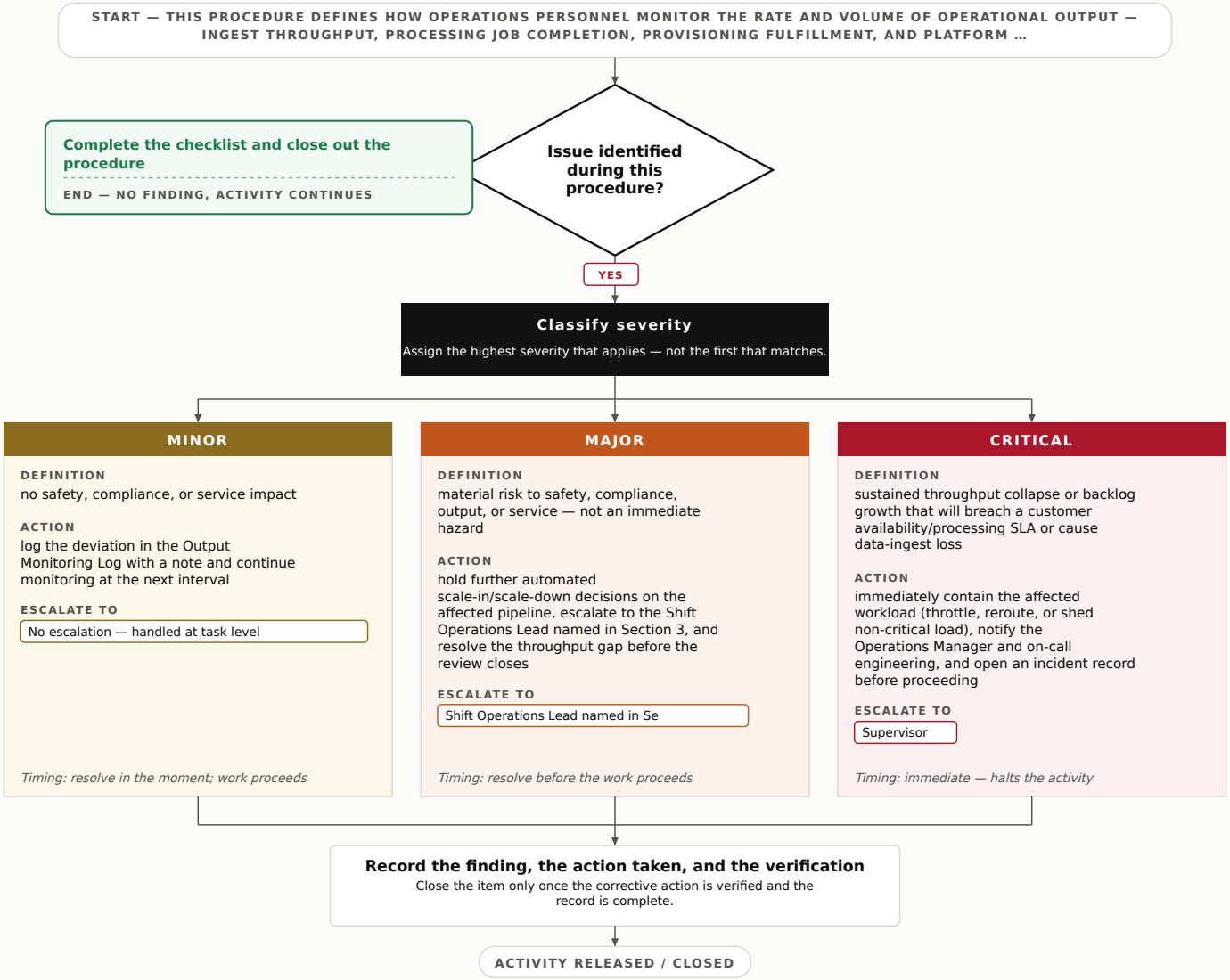

## 7. Step-by-Step Procedure

1. At the start of each defined review window, open the throughput dashboard and confirm all telemetry feeds (ingest, processing queue depth, provisioning fulfillment, request rate) are live and current.
2. Retrieve interval actuals: records/sec ingested, batch/stream job completion count, provisioning tickets fulfilled, and peak/sustained request rate.
3. Compare each actual against the planned target and expected range from the current capacity baseline.
4. Calculate deviation (percent above/below plan) and note any sustained trend across the trailing intervals (e.g., queue depth climbing, completion rate falling).
5. Flag any metric outside its expected range and check for correlated causes (upstream feed stall, node saturation, backlog growth).
6. Classify each flagged deviation per the Decision Tree (Section 8) and route accordingly.
7. Confirm no throughput deviation is masking an SLA-relevant service impact; hand off any capability-driven concern to QC-026 rather than analyzing it here.
8. Record all metrics, deviations, classifications, and actions in the Output Monitoring Log with timestamp and reviewer initials.

## 8. Decision Tree

OD-014 · OPERATIONS · DATA HOSTING

## Decision Tree — Output Monitoring & Throughput Review




READING THIS TREE

- **No finding** — Activity stands. Complete the checklist and continue.
- **Minor** — Handled in place at task level; no escalation.
- **Major** — Supervisory decision required before the next stage.
- **Critical** — Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- All telemetry feeds confirmed live and current before metrics are read.
- Every metric compared against its documented plan target, not a remembered or assumed value.
- All flagged deviations classified and routed with a recorded action.
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| Telemetry feeds live and current for all monitored streams | | |
| Ingest rate within planned range | | |
| Processing/batch job completion rate meets plan | | |
| Provisioning fulfillment volume on target | | |
| Request rate within capacity headroom | | |
| Queue depth / backlog trend stable or declining | | |
| All deviations classified, routed, and logged | | |

## 11. KPIs

- Percentage of review intervals completed on schedule ≥ 98%
- Throughput actuals within ±10% of plan across monitored streams ≥ 95% of intervals
- Time from Critical deviation detection to containment ≤ 15 minutes

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# OD-015 — Bottleneck Identification & Response

**Estimated completion time: 30–90 minutes per identified constraint (excluding downstream remediation)**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

Detect and respond to operational constraints — compute, storage I/O, network, power, cooling, or ticket-queue backlog — that are slowing hosted-service throughput, so that customer SLAs are protected and degradation is contained before it cascades.

## 2. Scope

Covers real-time and trend-based bottleneck detection across production hosting infrastructure and the Operations queue, plus first-response containment and escalation. Excludes shift/schedule reallocation (see OD-017) and capacity allocation or provisioning decisions (see OD-009).

## 3. Responsibilities

- NOC Operator — monitors dashboards and alert thresholds, triages first-response, logs each constraint event.
- Operations Shift Lead — classifies severity, authorizes containment actions, escalates Major/Critical events.
- Infrastructure Reliability Engineer — validates root-cause telemetry and confirms remediation before closeout.

## 4. Required PPE & Lockout/Tagout

- Standard facility PPE for data-hall entry (ESD wrist strap, closed-toe footwear, hearing awareness in high-airflow zones); primarily a console/monitoring task.
- Not applicable to the analysis task — no hazardous energy involved. Any physical hardware swap arising from findings follows the facility LOTO procedure and is out of scope here.

## 5. Regulatory References

- None sector-specific mandate bottleneck response; internal Operations policy and customer SLA contracts apply. Supporting frameworks: SOC 2 (AICPA TSC — Availability) and ISO/IEC 27001:2022 A.8 (operational monitoring/capacity) where the facility is certified; NFPA 70/70E for any electrical constraint referral.
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow

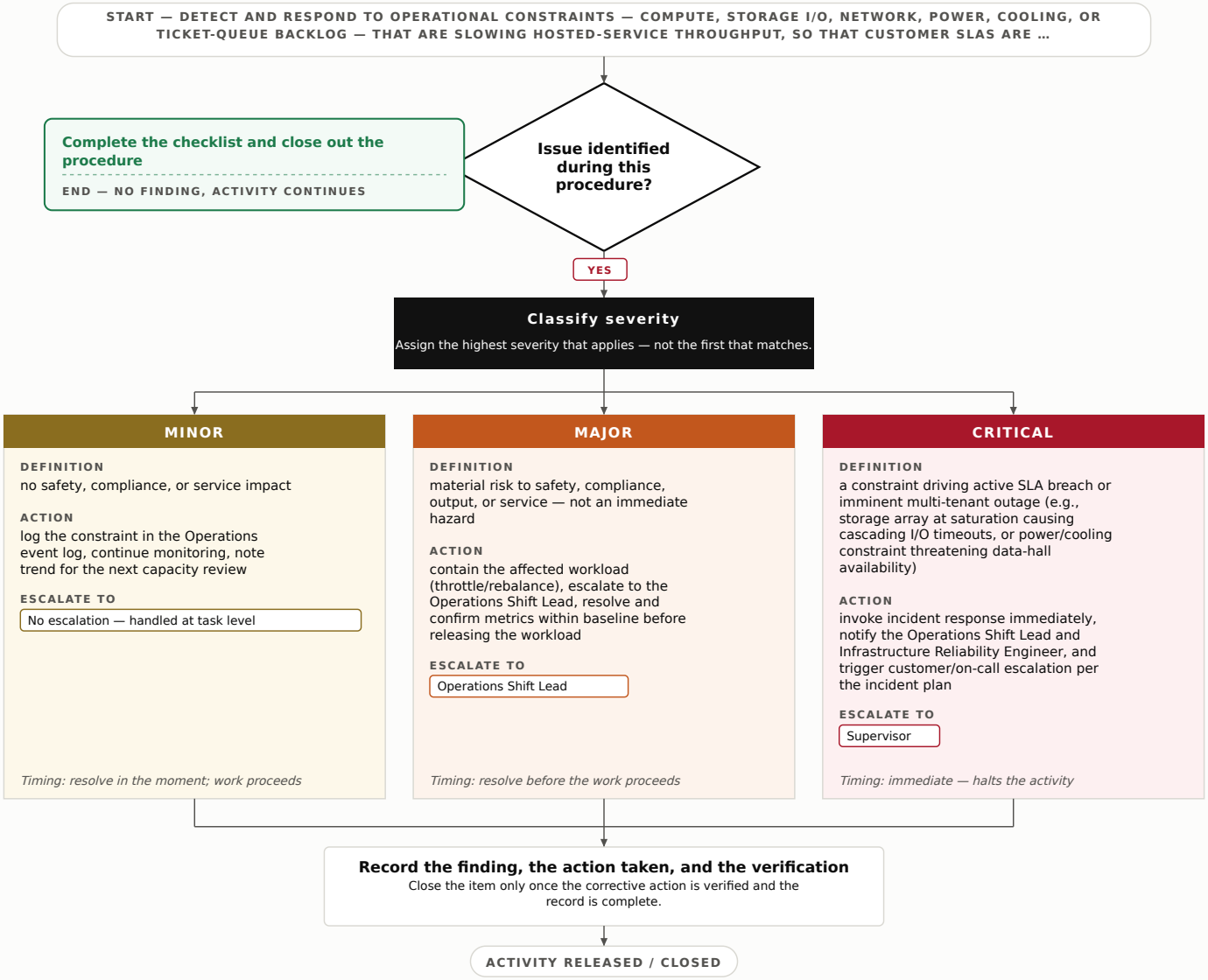

## 7. Step-by-Step Procedure

1. Confirm monitoring coverage is live — verify DCIM, hypervisor, storage-array, network, and ticket-queue dashboards are reporting current data with no stale sensors.
2. Compare live metrics against established baselines: CPU-ready %, storage IOPS/latency, network utilization and packet loss, PDU/branch load, CRAC return-air temp, and Ops ticket age.
3. Identify the constraining resource — pinpoint the single stage where throughput is capped (e.g., storage latency spike, saturated uplink, backlogged provisioning queue).
4. Quantify impact — determine affected tenants/services and current or projected SLA exposure.
5. Classify severity using the Decision Tree (Section 8).
6. Apply first-response containment appropriate to the constraint (e.g., throttle non-critical batch jobs, rebalance traffic, reprioritize queue — without reallocating capacity per OD-009).
7. Escalate per severity and hand off to the Infrastructure Reliability Engineer for root-cause validation where required.
8. Document the event: constraint type, metrics, impact, action taken, timestamps, and resolution status in the Operations event log.

## 8. Decision Tree

OD-015 · OPERATIONS · DATA HOSTING

## Decision Tree — Bottleneck Identification & Response




### READING THIS TREE

**No finding**
Activity stands. Complete the checklist and continue.

**Minor**
Handled in place at task level; no escalation.

**Major**
Supervisory decision required before the next stage.

**Critical**
Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- Baselines and alert thresholds confirmed current before analysis begins.
- Constraining stage correctly isolated and quantified against SLA terms.
- Containment action verified to move the metric back within baseline.
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| Monitoring dashboards live, no stale sensors | | |
| Live metrics compared to documented baselines | | |
| Constraining resource isolated to single stage | | |
| Tenant/SLA impact quantified | | |
| Severity classified per Section 8 | | |
| Containment action applied and metric re-checked | | |
| Event logged with timestamps and status | | |

## 11. KPIs

- Mean time to detect (MTTD) constraint from onset: ≤ 5 minutes.
- Constraint events contained before SLA breach: ≥ 95%.
- Event-log completeness (all required fields captured): 100%.

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# OD-016 — Rework & Nonconforming Work Handling

**Estimated completion time: 1–4 hours per nonconforming work item (excludes queued re-run duration)**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

This procedure establishes how Operations segregates, contains, and re-runs data-hosting work — such as failed batch processing jobs, incomplete backups, corrupt migration transfers, or provisioning tasks that miss SLA/spec — so that nonconforming output does not reach the customer or downstream systems. It protects data integrity and service continuity while a clean re-run is produced.

## 2. Scope

Covers identification, quarantine, tagging, and re-execution of nonconforming operational work (jobs, transfers, provisioned resources, and outputs) within the OD environment. Excludes formal disposition decisions, which are covered under QC-014, and rework authorization sign-off, which is covered under QC-016.

## 3. Responsibilities

- Operations Shift Lead — confirms nonconformance, orders containment, assigns and schedules the re-run, and owns closeout.
- Hosting Operations Technician — segregates the affected job/output, applies quarantine tags, executes the approved re-run, and records evidence.
- Service Delivery Coordinator — tracks SLA/customer impact and coordinates any required customer or QC hand-off.

## 4. Required PPE & Lockout/Tagout

- Standard facility PPE for data-center floor access (ESD wrist strap and closed-toe footwear when handling physical storage media from 334112 suppliers); none required for console-only work.
- Not applicable — no hazardous energy involved. Logical containment (job hold, resource isolation, write-lock) replaces physical LOTO.

## 5. Regulatory References

- SOC 2 (AICPA TSC) — Processing Integrity and Availability criteria governing complete, valid, and accurate processing.
- ISO/IEC 27001:2022 A.5.24 / A.8.15 (information security incident and logging controls).
- Contractual/regulatory data obligations as applicable (e.g., GDPR Art. 32, HIPAA Security Rule 45 CFR §164.312 where PHI is hosted).
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow

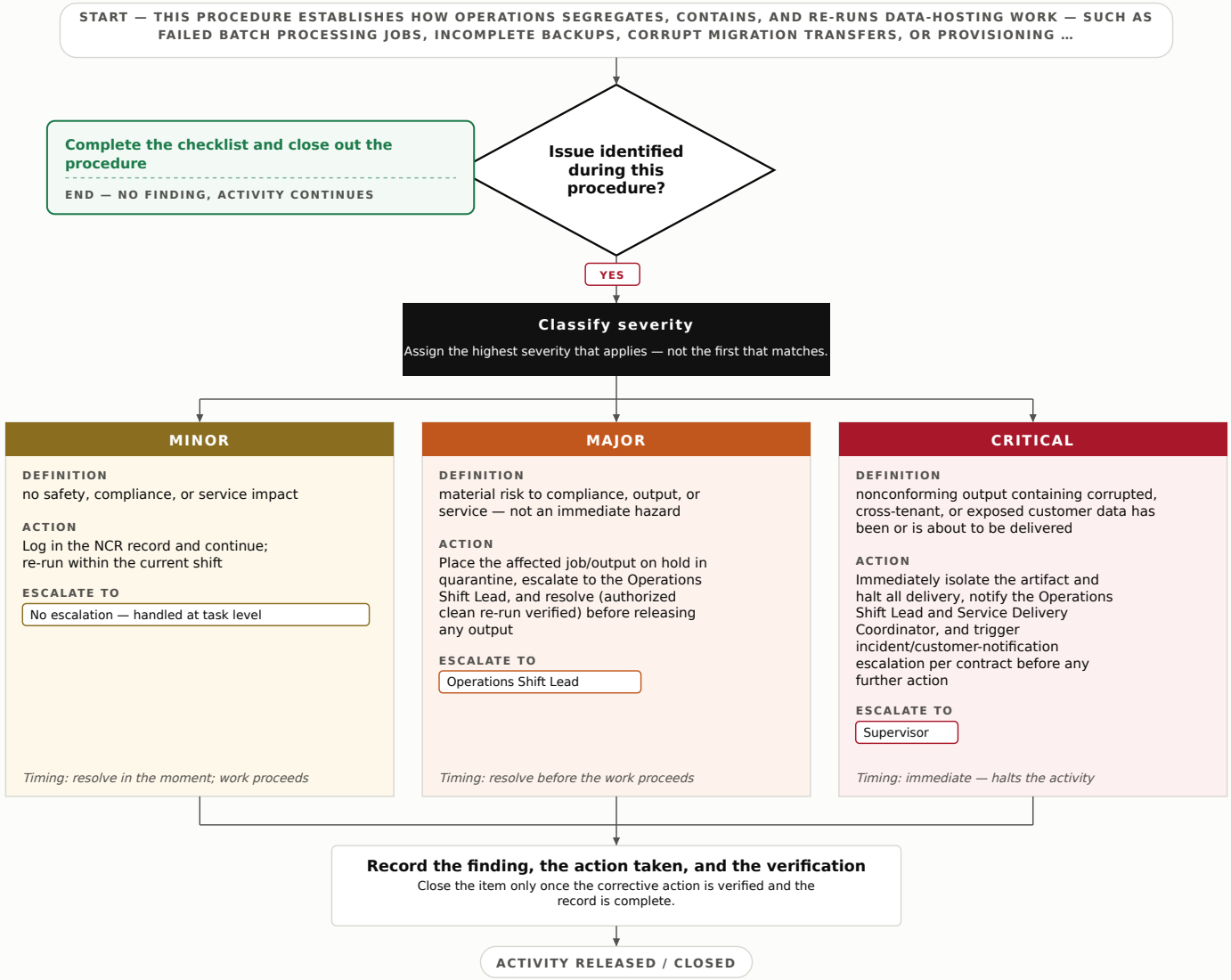

## 7. Step-by-Step Procedure

1. Upon detecting a failed or out-of-spec job/output (monitoring alert, checksum mismatch, SLA miss, corrupt transfer), halt any downstream consumption of that output immediately.
2. Segregate the affected artifact — move it to the quarantine namespace/storage path or apply a write-lock/hold so it cannot be delivered or overwritten.
3. Apply a nonconformance tag: record job ID, timestamp, system, customer/tenant, and failure symptom in the NCR log.
4. Assess scope and impact with the Service Delivery Coordinator — identify affected tenants, data ranges, and SLA exposure.
5. Confirm rework authorization per QC-016 before re-executing; do not re-run un-authorized work.
6. Preserve the original nonconforming artifact (do not delete) for QC-014 disposition; execute the re-run against a clean input source on validated infrastructure.
7. Verify the re-run output against spec (checksum, record count, integrity checks); release to the customer/downstream channel only on pass.
8. Document the full chain — detection, containment, authorization reference, re-run result, and release — in the NCR log and close the item.

## 8. Decision Tree

OD-016 · OPERATIONS · DATA HOSTING

## Decision Tree — Rework & Nonconforming Work Handling




READING THIS TREE

- **No finding** — Activity stands. Complete the checklist and continue.
- **Minor** — Handled in place at task level; no escalation.
- **Major** — Supervisory decision required before the next stage.
- **Critical** — Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- Affected output confirmed segregated and unreachable by downstream/customer before re-run begins.
- Rework authorization reference (QC-016) recorded prior to re-execution.
- Re-run output passes integrity/spec verification (checksum, record count) before release.
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| Nonconforming job/output identified and quarantined | | |
| NCR log entry created with job ID, tenant, and symptom | | |
| Impact/SLA assessment completed with Service Delivery | | |
| Rework authorization confirmed per QC-016 | | |
| Original artifact preserved for QC-014 disposition | | |
| Re-run output verified against spec before release | | |
| Closeout documented in NCR log | | |

## 11. KPIs

- Nonconforming output reaching customer: 0 per quarter.
- Re-run first-pass success rate: ≥ 95%.
- Mean time to containment after detection: ≤ 30 minutes.

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# OD-017 — Schedule Deviation & Change Management

**Estimated completion time: 30–90 minutes per change event (excluding downstream execution)**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

Establish a controlled method for capturing, classifying, and authorizing deviations to scheduled Operations work — maintenance windows, migration cutovers, provisioning tickets, and capacity builds — so committed SLAs and change-window obligations are preserved when timelines, priorities, or dependencies shift.

## 2. Scope

Covers all schedule deviations, change requests, delays, and priority re-sequencing affecting Operations-owned work orders and maintenance windows in the hosting environment, from intake through authorization and record close. Excludes bottleneck root-cause response (see OD-015) and customer/tenant notification (see OD-022), which are authored in their own modules.

## 3. Responsibilities

- Change & Scheduling Coordinator — logs deviations, maintains the change calendar, classifies impact, and drives approvals within the change window.
- Operations Shift Lead — assesses operational and SLA impact, approves or holds Minor/Major changes, and executes re-sequencing on the floor.
- Operations Manager (Change Authority) — authorizes Major and Critical changes, owns emergency change decisions, and signs off on commitment impacts.

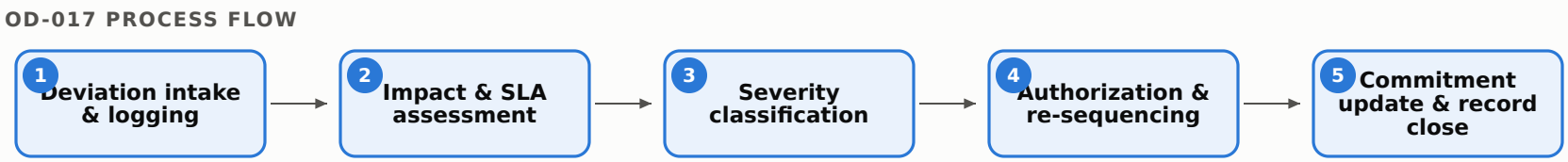
## 4. Required PPE & Lockout/Tagout

- Standard facility PPE for any data-hall entry (ESD wrist strap, closed-toe footwear); administrative task otherwise performed at the NOC/console.
- Not applicable — no hazardous energy involved; this is a coordination and records task. Physical energy isolation for affected equipment is governed by the relevant maintenance SOP.

## 5. Regulatory References

- SOC 2 (AICPA TSC) change-management and availability criteria; ISO/IEC 27001:2022 A.8.32 (Change Management); contractual SLA and Master Service Agreement change-window terms; internal Operations Change Management Policy.
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow



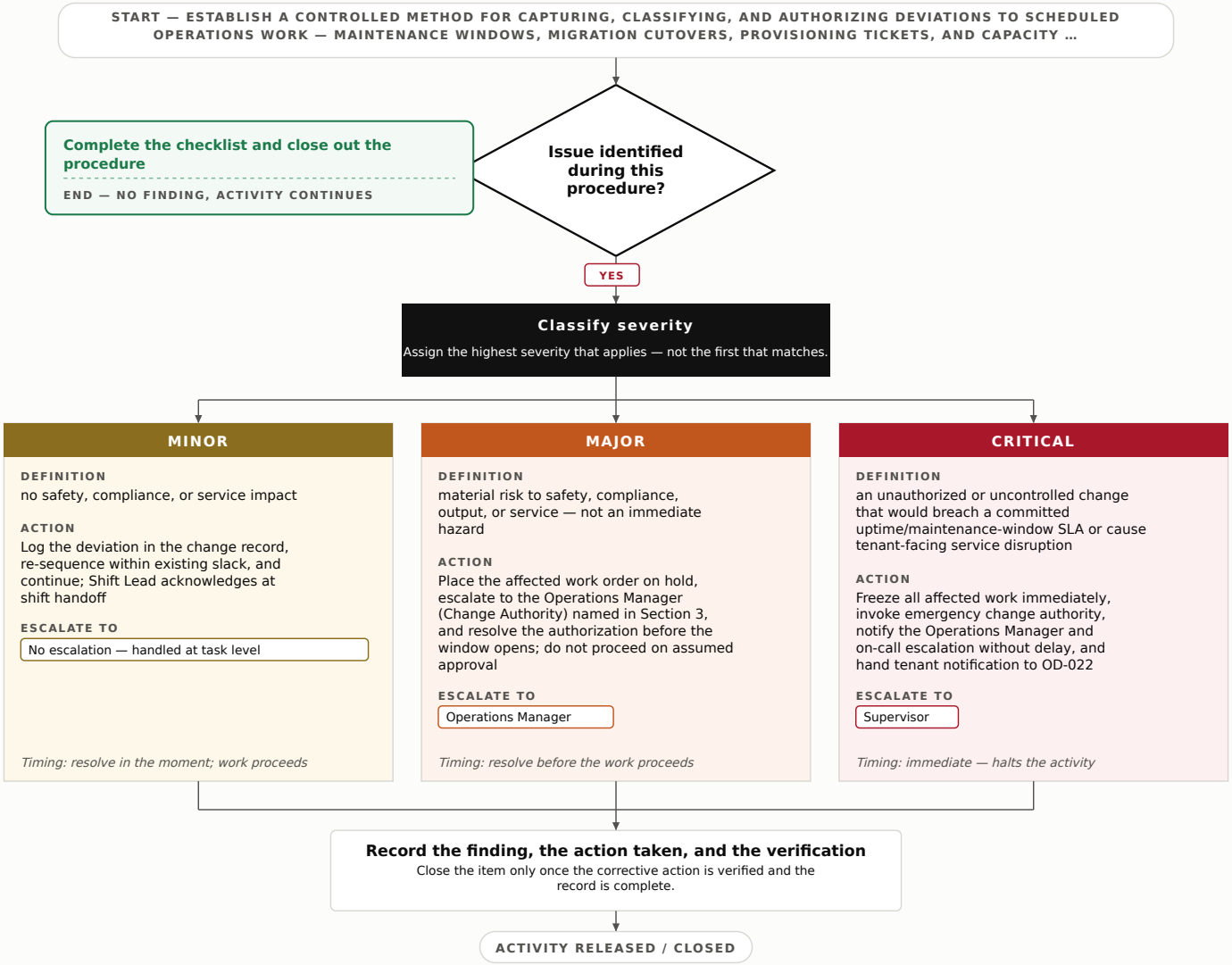

## 7. Step-by-Step Procedure

1. Capture the deviation in the change management system with a unique change ID, affected work order(s), requested timing shift, and originating trigger (delay, priority shift, dependency slip, emergency).
2. Identify all impacted commitments — active SLAs, contractual maintenance windows, migration cutover deadlines, and dependent provisioning tickets from the affected rack/tenant.
3. Assess collision risk against the change calendar: verify the requested window does not overlap a freeze period, another tenant's approved window, or a hardware delivery dependency (see Section on vendor touchpoints).
4. Classify severity using the Decision Tree (Section 8) based on safety, compliance, output, and service consequence.
5. Route for authorization: Shift Lead for Minor/Major re-sequencing within tolerance; Operations Manager for Major SLA-affecting or Critical/emergency changes.
6. On approval, update the change calendar and dependent work orders; hand off any required tenant messaging to OD-022 and any root-cause containment to OD-015.
7. Confirm revised commitment dates back into the SLA tracker and mark the original schedule entry superseded (never deleted) for audit traceability.
8. Document the full decision trail — requester, impact assessment, approver, revised timing, and residual risk — and close the change record.

## 8. Decision Tree

OD-017 · OPERATIONS · DATA HOSTING

## Decision Tree — Schedule Deviation & Change Management




**READING THIS TREE**

- **No finding** — Activity stands. Complete the checklist and continue.
- **Minor** — Handled in place at task level; no escalation.
- **Major** — Supervisory decision required before the next stage.
- **Critical** — Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- Every deviation has a unique change ID and named requester before assessment begins.
- Impact assessment lists all affected SLAs and dependent work orders, verified against the live change calendar.
- Authorization level matches classified severity; no Major/Critical change executed without documented approver sign-off.
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| Change ID logged with originating trigger recorded | | |
| Affected SLAs and dependent work orders identified | | |
| Change calendar checked for freeze/window collisions | | |
| Severity classified per Decision Tree | | |
| Approval captured at correct authority level | | |
| Revised commitment dates written back to SLA tracker | | |
| Original schedule entry superseded, not deleted (audit trail intact) | | |

## 11. KPIs

- Deviations logged with complete impact assessment ≥ 98%
- Changes authorized at correct severity level before execution 100%
- SLA/maintenance-window breaches resulting from uncontrolled change 0 per quarter

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# OD-018 — Subcontractor & Vendor Coordination

**Estimated completion time: 45–90 minutes per vendor engagement cycle; 2–4 hours for a new onboarding**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

Establish a repeatable method for engaging, scheduling, and tracking external providers — smart-hands technicians, hardware installers, network carriers, and equipment resellers — who perform part of a data hosting operation, so that colocation and hosting services continue to meet customer SLAs and access-control commitments.

## 2. Scope

Covers the intake, authorization, scheduling, work-order handoff, and closeout of subcontractor and vendor activity within the data center white space and staging areas of the Operations department. Excludes contractor maintenance supervision, which is covered under MD-018, and contractor safety and hazard controls, which are covered under SD-023.

## 3. Responsibilities

- Operations Coordinator — issues vendor work orders, verifies scope against the customer SLA, and maintains the vendor coordination log.
- Data Center Operations Manager — approves vendor scope, authorizes escorted white-space access, and owns escalation decisions.
- Security/Access Control Officer — validates vendor credentials, badges, and NDA/DPA status before any physical or logical access is granted.

## 4. Required PPE & Lockout/Tagout

- Standard facility PPE for staged escort into white space (ESD wrist strap when handling live equipment, closed-toe footwear). Coordination itself is largely administrative.
- Not applicable — no hazardous energy is controlled by this procedure; any LOTO required for physical work is handled under MD-018/SD-023.

## 5. Regulatory References

- SOC 2 Trust Services Criteria (AICPA) — vendor management / CC9.2 subservice-organization controls
- NIST SP 800-53 Rev. 5 SA-9 (External System Services) and PS-7 (Third-Party Personnel Security)
- Contractual DPA obligations under applicable privacy regimes (e.g., GDPR Art. 28 processor terms) where customer data is in scope
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow

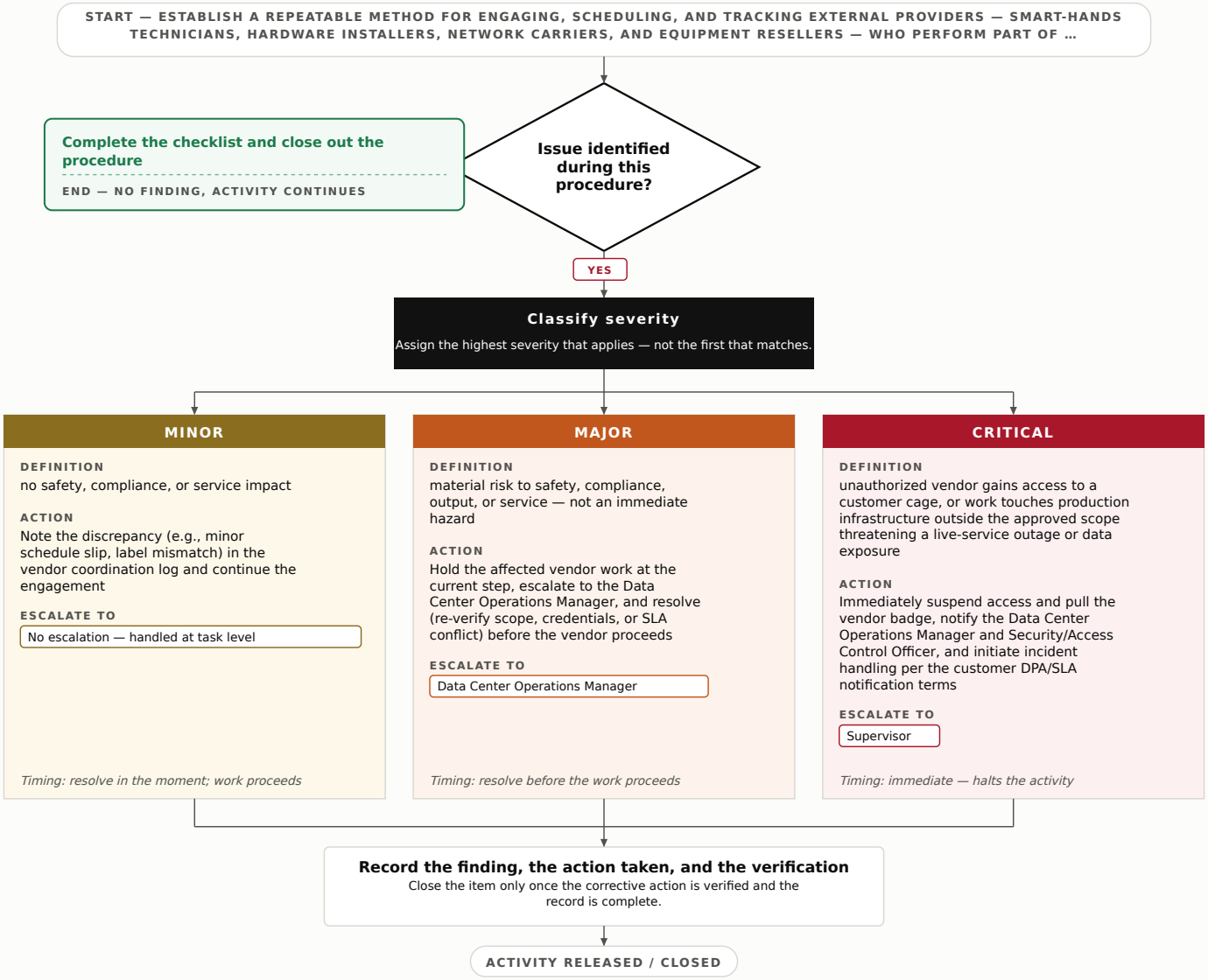

## 7. Step-by-Step Procedure

1. Receive the vendor/subcontractor request and record the requesting customer or internal owner, the affected racks/cages, and the target SLA window in the vendor coordination log.
2. Confirm scope: verify the requested work (e.g., hardware install from a 423430 reseller, carrier cross-connect, storage device swap) matches an approved change ticket and does not conflict with an active maintenance window (cross-check MD-018).
3. Route credentials to the Security/Access Control Officer to validate vendor identity, current NDA/DPA execution, and insurance/COI on file.
4. Obtain Data Center Operations Manager approval for white-space access scope and escort level (escorted vs. monitored).
5. Schedule the engagement against the SLA window; issue the vendor work order with defined cage/rack IDs, permitted actions, and start/stop times.
6. Hand off to the escort at check-in: verify badge issuance, confirm the vendor understands the work boundary, and record time-in.
7. On completion, walk the affected racks with the vendor to confirm work matches the order, collect any equipment serials or cross-connect labels, and record time-out and badge return.
8. Document the completed engagement, attach the signed work order and any delivery/receiving records, and close the entry in the vendor coordination log.

## 8. Decision Tree

OD-018 · OPERATIONS · DATA HOSTING

## Decision Tree — Subcontractor & Vendor Coordination




READING THIS TREE

- **No finding** — Activity stands. Complete the checklist and continue.
- **Minor** — Handled in place at task level; no escalation.
- **Major** — Supervisory decision required before the next stage.
- **Critical** — Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- Vendor scope matches an approved change ticket and current customer SLA window before scheduling.
- NDA/DPA, COI, and credential validation confirmed by the Security/Access Control Officer prior to any access.
- Work-order completion verified against physical rack state at closeout, with serials/labels captured.
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| Vendor request tied to an approved change ticket | | |
| NDA/DPA and COI current and on file | | |
| Credentials validated by Security/Access Control Officer | | |
| DC Operations Manager access-scope approval recorded | | |
| Work order specifies cage/rack IDs and permitted actions | | |
| Time-in / time-out and badge return logged | | |
| Completed work matches order; serials/labels captured | | |

## 11. KPIs

- Vendor engagements completed within scheduled SLA window ≥ 98%
- Vendor access events with fully verified credentials before entry = 100%
- Vendor coordination log entries closed with completed work order within 24 hours ≥ 95%

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# OD-019 — Interdepartmental Coordination Review

**Estimated completion time: 60–90 minutes per review cycle**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

This procedure aligns Operations with the other departments touching the same hosting work — Provisioning, Network/Security, Facilities, and Customer Success — so that data center changes, capacity moves, and customer commitments are coordinated before execution. It prevents conflicting change windows, capacity conflicts, and unacknowledged SLA impacts across the same rack, tenant, or workload.

## 2. Scope

Covers the recurring cross-department coordination review for shared hosting work: change calendar reconciliation, capacity and power/cooling dependencies, SLA/maintenance-window alignment, and hand-off confirmation across OD-adjacent teams. Self-contained within OD as a cross-department coordination overview; it does not author the detailed procedures, checklists, or KPIs of the referenced departments — those live in their own modules.

## 3. Responsibilities

- Operations Coordination Lead (OD) — chairs the review, owns the shared change calendar, reconciles conflicts, and records the outcome.
- Shift Operations Manager (OD) — confirms floor capacity, power/cooling headroom, and staffing for coordinated work windows.
- Department Liaisons (Provisioning, Network/Security, Facilities, Customer Success) — each represents their department's committed work, dependencies, and customer-facing impacts.

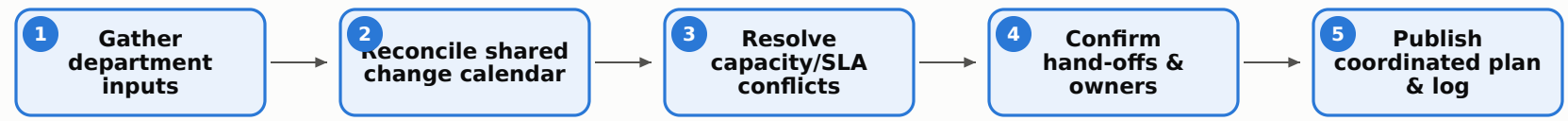
## 4. Required PPE & Lockout/Tagout

- Standard facility PPE only if the review is conducted on the data hall floor; conference/remote review requires none.
- Not applicable — no hazardous energy involved (coordination/administrative task; any physical work is executed under its own department module).

## 5. Regulatory References

- SOC 2 (AICPA TSC) change-management and availability criteria; ISO/IEC 27001:2022 Annex A change and capacity controls; applicable customer contractual SLAs and data-processing agreements. None additional sector-specific for coordination itself; internal Operations change-coordination policy applies.
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow



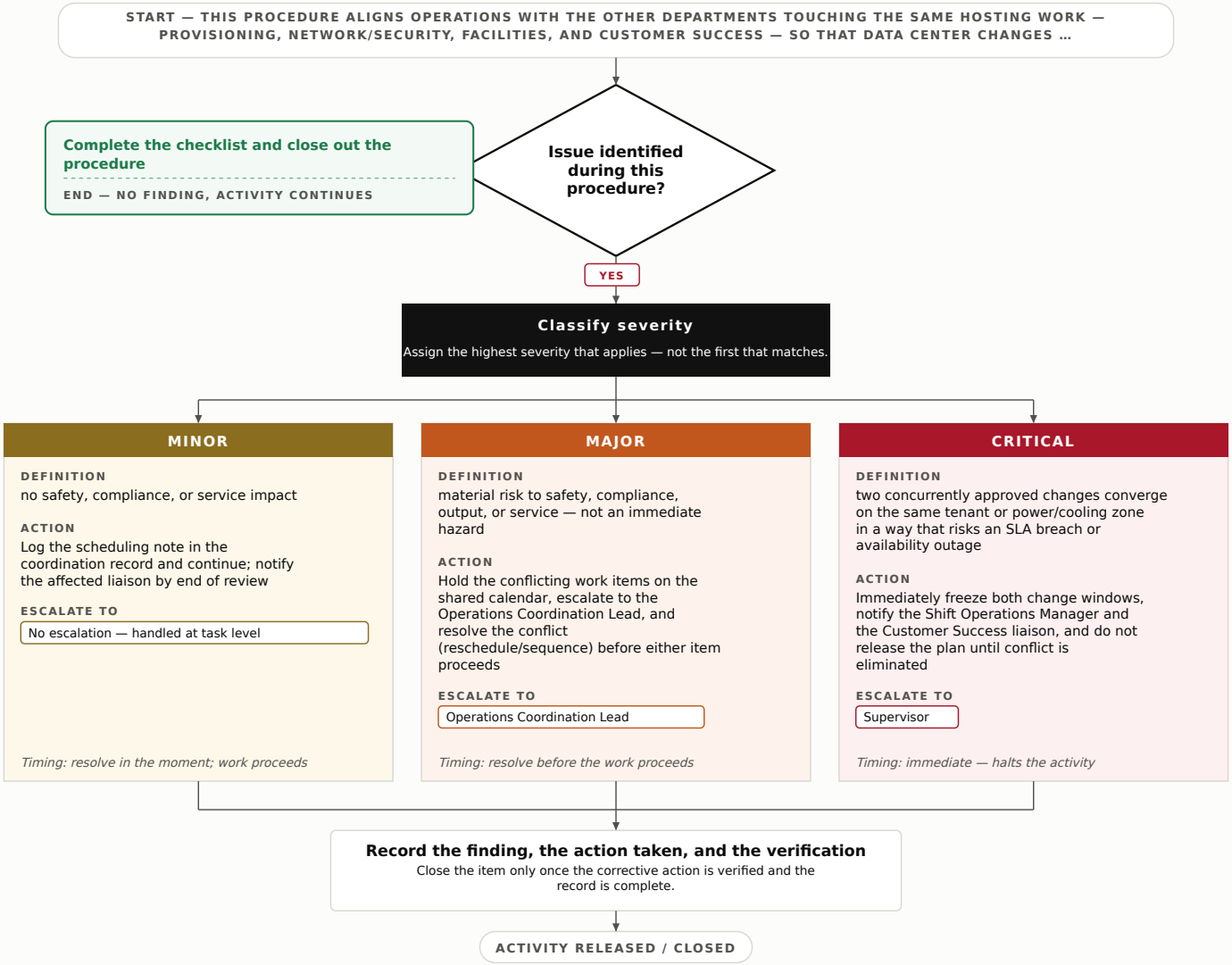

## 7. Step-by-Step Procedure

1. Collect each department's proposed work touching shared racks, tenants, network segments, or power/cooling zones for the review horizon (typically next 7–14 days).
2. Overlay all items on the shared change calendar and flag any that share the same rack, tenant, maintenance window, or power/cooling zone.
3. For each flagged overlap, confirm capacity and power/cooling headroom with the Shift Operations Manager before both items are allowed to proceed together.
4. Verify every customer-impacting item has an aligned maintenance window and that any SLA impact is acknowledged by the Customer Success liaison.
5. Resolve conflicts by sequencing, rescheduling, or splitting windows; record the agreed decision and the accountable owner for each item.
6. Confirm hand-off points between departments (e.g., provisioning complete before network cutover) and name the receiving role for each.
7. Obtain verbal or written concurrence from each department liaison on the reconciled plan.
8. Publish the coordinated plan to the shared calendar and log the review outcome, decisions, owners, and any unresolved items in the coordination record.

## 8. Decision Tree

OD-019 · OPERATIONS · DATA HOSTING

## Decision Tree — Interdepartmental Coordination Review




**READING THIS TREE**

- **No finding** — Activity stands. Complete the checklist and continue.
- **Minor** — Handled in place at task level; no escalation.
- **Major** — Supervisory decision required before the next stage.
- **Critical** — Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- Every shared-resource overlap on the calendar has a documented resolution and named owner.
- All customer-impacting items have an acknowledged maintenance window and SLA impact confirmation.
- Each cross-department hand-off has a named receiving role and sequencing dependency.
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| All department inputs collected for review horizon | | |
| Shared calendar overlaps flagged and reviewed | | |
| Capacity / power-cooling headroom confirmed for concurrent work | | |
| Customer-impacting items have aligned maintenance windows | | |
| Hand-off points and receiving owners documented | | |
| Liaison concurrence obtained from each department | | |
| Coordinated plan published and review logged | | |

## 11. KPIs

- Cross-department change conflicts reaching execution: 0 per cycle.
- Coordinated review completed on schedule: ≥ 98% of scheduled cycles.
- Customer-impacting items with confirmed SLA acknowledgement before window: 100%.

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# Phase 4 — Completion & customer handoff

# OD-020 — Job / Order Completion Verification

**Estimated completion time: 30–60 minutes per provisioning order or service turnover**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

This procedure confirms that a completed hosting provisioning job or service order — server build-out, storage allocation, tenant migration, or managed-service turn-up — matches the signed order specification and SLA before it moves to formal release. It prevents mis-provisioned or incomplete environments from reaching the customer.

## 2. Scope

Covers verification that all line items of a completed provisioning/service order (compute, storage, network, access, monitoring hooks) are present, configured to the order spec, and documented. Excludes final inspection, which is covered under QC-012, and formal customer release/sign-off, which is covered under QC-013.

## 3. Responsibilities

- Provisioning Technician (OD) — assembles the completion evidence, runs the verification checks against the order spec, records results.
- Operations Lead (OD) — reviews findings, adjudicates Major/Critical issues, authorizes progression to QC-012.
- Service Delivery Coordinator (OD) — reconciles the verified order against the customer contract and SLA line items, maintains the order record.

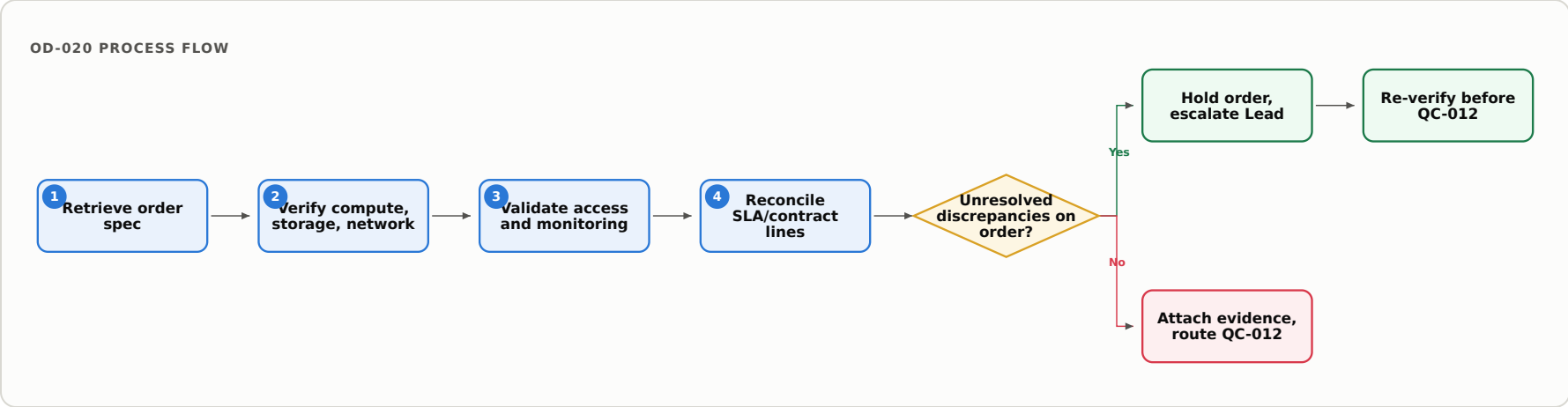
## 4. Required PPE & Lockout/Tagout

- Standard facility PPE for data-hall entry when physically verifying rack-mounted hardware (ESD wrist strap, closed-toe footwear); none required for remote/console verification.
- Not applicable — no hazardous energy involved. Physical rack hardware is verified in an energized production state; do not open PDUs or power infrastructure under this task.

## 5. Regulatory References

- SOC 2 (AICPA TSC) change-management and processing-integrity criteria; ISO/IEC 27001 Annex A (A.8 asset/config, A.12 operations); PCI-DSS Req. 2 & 6 where cardholder-data tenants apply; customer contract/SLA terms.
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow



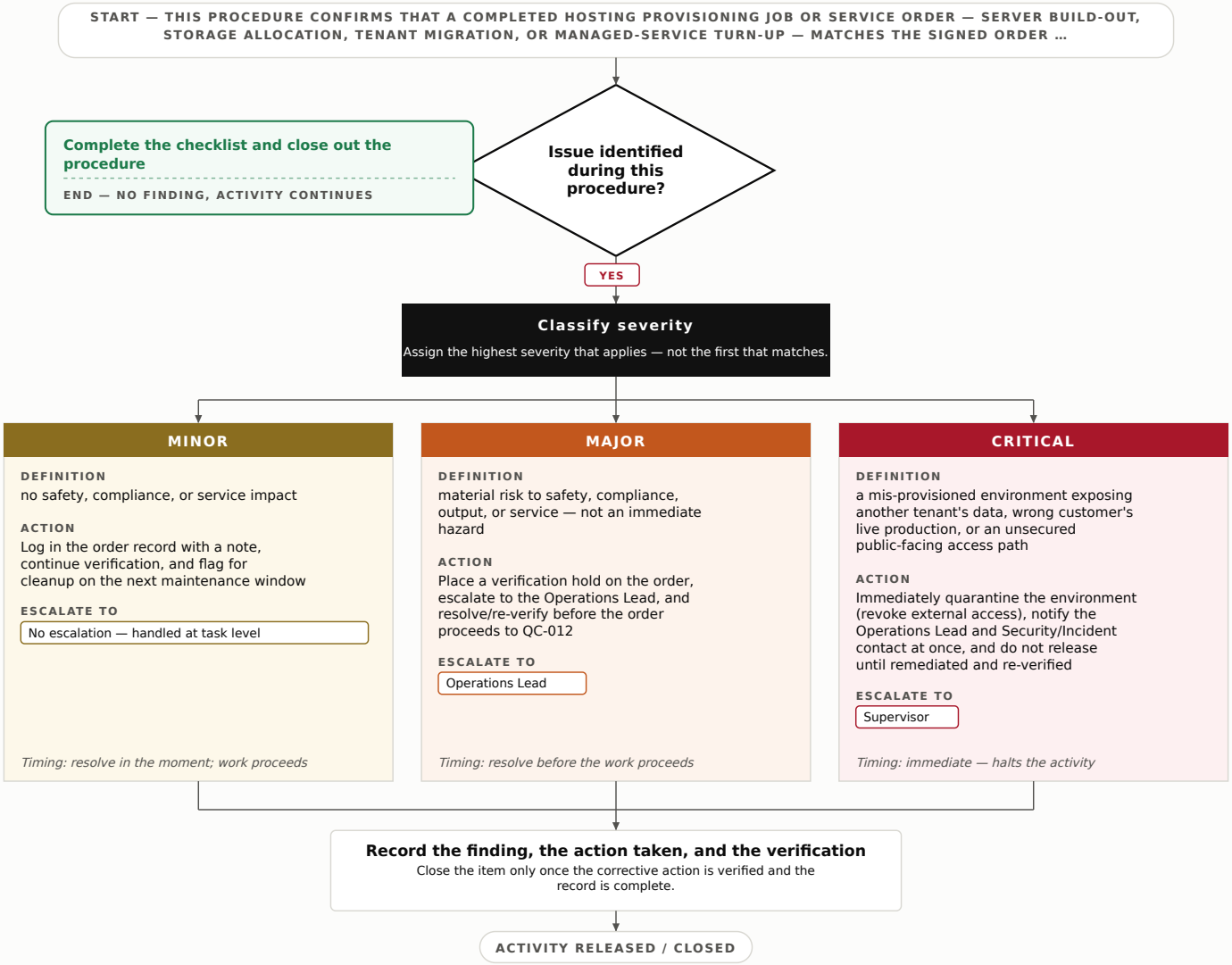

## 7. Step-by-Step Procedure

1. Retrieve the signed order/work ticket and the technician's completion record; confirm the ticket is marked "build complete" and all sub-tasks closed.
2. Verify provisioned compute and storage match the spec — CPU/RAM allocation, storage tier and capacity, hostnames, and asset tags against ordered hardware (see 334111/334112 supply records where new units were deployed).
3. Confirm network configuration — VLAN/subnet assignment, IP allocation, firewall/security-group rules, and DNS entries match the order.
4. Validate access controls — tenant/user accounts, RBAC roles, and credential handover method are provisioned exactly as specified; confirm no default or unauthorized accounts remain.
5. Confirm monitoring, backup, and alerting hooks are active and reporting (agent check-in, backup schedule attached, SLA-linked alert thresholds set).
6. Reconcile every verified item line-by-line against the customer contract and SLA parameters with the Service Delivery Coordinator; flag any gaps.
7. Classify any discrepancies using Section 8; hold the order if unresolved.
8. Record verification results, attach evidence (config exports, screenshots, asset-tag scans) to the order record, and route the completed package to final inspection per QC-012.

## 8. Decision Tree

OD-020 · OPERATIONS · DATA HOSTING

## Decision Tree — Job / Order Completion Verification




READING THIS TREE

- **No finding** — Activity stands. Complete the checklist and continue.
- **Minor** — Handled in place at task level; no escalation.
- **Major** — Supervisory decision required before the next stage.
- **Critical** — Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- Every order line item mapped to a verified configuration item — no unmatched lines.
- Access controls and monitoring confirmed active before order progresses.
- SLA/contract reconciliation signed off by the Service Delivery Coordinator.
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| Compute/storage allocation matches order spec | | |
| Network config (VLAN, IP, firewall, DNS) verified | | |
| Access controls & RBAC provisioned per spec; no default accounts | | |
| Monitoring, backup & alerting active and reporting | | |
| Asset tags reconciled to deployed hardware | | |
| SLA/contract line items reconciled | | |
| Evidence attached to order record | | |

## 11. KPIs

- Order completion-verification accuracy (verified items matching spec at first pass) ≥ 98%
- Verification cycle time per order ≤ 60 minutes
- Orders reaching QC-012 with unresolved Critical findings = 0

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# OD-021 — Delivery / Service Turnover

**Estimated completion time: 30–90 minutes per turnover event**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

Formally release a provisioned hosting environment or managed service (virtual instances, storage allocations, network configuration, and access credentials) to the customer or the receiving distribution partner, confirming the delivered environment matches the signed service order before the customer assumes operational control.

## 2. Scope

Covers the final turnover of a completed hosting/service build to the customer or downstream channel — environment readiness confirmation, credential handoff, acceptance sign-off, and turnover documentation. Excludes physical loading/dispatch of hardware, which is covered under SH-014, and proof of delivery capture, which is covered under SH-024.

## 3. Responsibilities

- Service Delivery Coordinator (OD) — leads the turnover event, confirms environment against the service order, and obtains customer acceptance.
- Hosting Operations Engineer (OD) — validates provisioning, connectivity, and monitoring integration prior to release.
- Operations Supervisor (OD) — verifies completeness, resolves escalations, and authorizes final release.

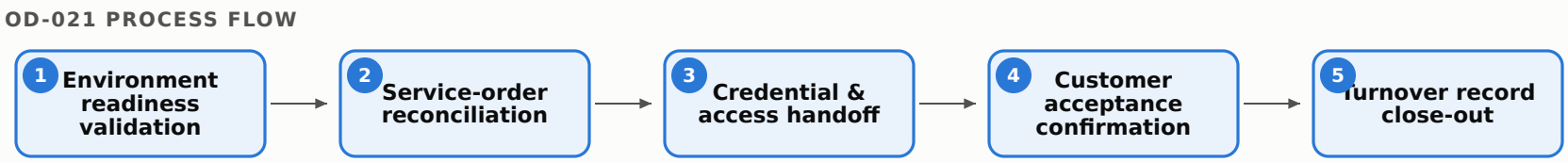
## 4. Required PPE & Lockout/Tagout

- Standard facility PPE if entering the data hall (ESD wrist strap, closed-toe footwear); none required for remote/console turnover.
- Not applicable — no hazardous energy involved. Access "lockout" is logical: revoke build-team elevated credentials at handoff.

## 5. Regulatory References

- SOC 2 (AICPA TSC) trust-services criteria for security, availability, and confidentiality of the turned-over environment.
- ISO/IEC 27001:2022 Annex A controls for information transfer and access provisioning.
- Contractual SLA / MSA terms and internal Service Turnover Policy (OD-POL-04) govern acceptance obligations.
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow



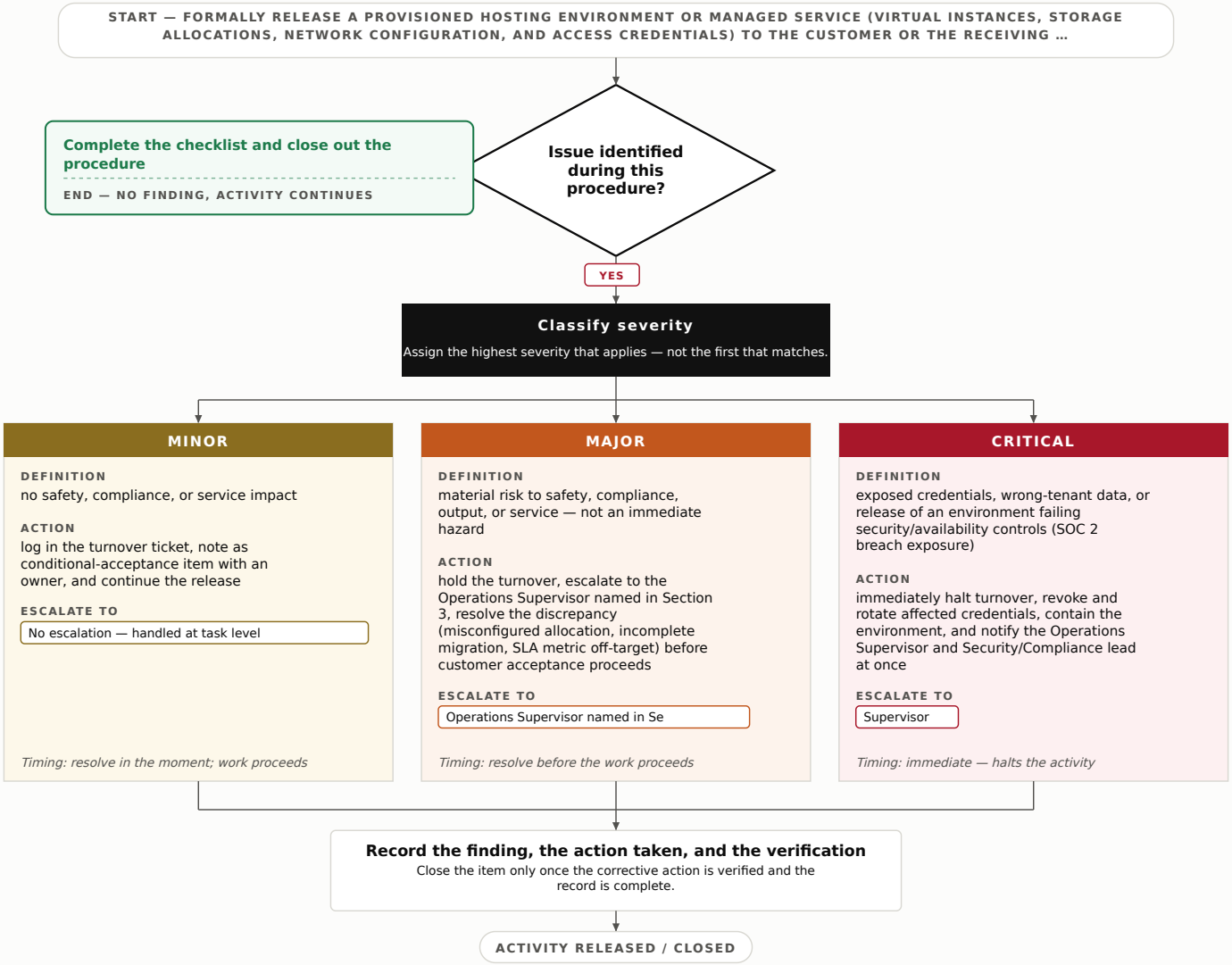

## 7. Step-by-Step Procedure

1. Retrieve the signed service order and provisioning ticket; confirm the environment scope (compute, storage tier, IP allocation, backup schedule) matches what was built.
2. Verify with the Hosting Operations Engineer that instances are live, monitoring/alerting is integrated, and SLA-relevant metrics (uptime, latency, backup success) report green.
3. Confirm data-migration or seed load (if in scope) completed and integrity checks passed; do not release on failed checks.
4. Prepare the credential package (admin access, API keys, connection endpoints) via the approved secure-transfer channel; revoke build-team elevated access.
5. Walk the customer or receiving channel partner (per 423430 Computer Equipment Wholesalers) through the delivered environment against the service order.
6. Obtain customer acceptance confirmation and note any conditional acceptance items with owners and dates.
7. Transition the account to production support / monitoring; notify the on-call and support queues of the go-live.
8. Record the turnover in the delivery log with timestamp, acceptance status, credential-transfer confirmation, and any open items; attach to the service ticket.

## 8. Decision Tree

OD-021 · OPERATIONS · DATA HOSTING

## Decision Tree — Delivery / Service Turnover




READING THIS TREE

- **No finding** — Activity stands. Complete the checklist and continue.
- **Minor** — Handled in place at task level; no escalation.
- **Major** — Supervisory decision required before the next stage.
- **Critical** — Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- Delivered environment reconciled line-by-line against the signed service order.
- Monitoring, alerting, and backup jobs confirmed active and reporting green.
- Credentials transferred via approved secure channel and build-team access revoked.
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| Service order matches provisioned environment | | |
| SLA metrics (uptime/latency/backup) reporting green | | |
| Data migration/integrity checks passed | | |
| Credentials issued via secure channel; build-team access revoked | | |
| Customer acceptance obtained (or conditional items logged) | | |
| Production support/monitoring transition confirmed | | |
| Turnover recorded in delivery log with timestamp | | |

## 11. KPIs

- On-time turnover vs. committed go-live date ≥ 95%.
- Turnover events released with zero post-handoff config defects ≥ 98%.
- Credential-handoff security incidents = 0.

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# OD-022 — Customer Communication & Status Notification

**Estimated completion time: 15–45 minutes per notification cycle; ongoing during active incidents**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

To keep hosting customers accurately and promptly informed of service status, scheduled maintenance, incidents, configuration changes, and completion of work orders, so that contractual SLA notification commitments are met and customer trust in the hosted environment is preserved.

## 2. Scope

Covers all outbound customer-facing status communications — maintenance windows, incident updates, RFOs (Reason for Outage), migration/provisioning completion, and change notifications — issued by Operations for hosted infrastructure and colocation services. Excludes complaint intake, which is covered under OD-023, and quality complaint investigation, which is covered under QC-021.

## 3. Responsibilities

- NOC Communications Coordinator — drafts, times, and issues status notifications per SLA windows; maintains the notification log.
- Operations Shift Lead — approves message content and severity classification before release; escalates Critical events.
- Customer Success Manager — owns account-level relationships, tailors messaging to affected tenants, and confirms receipt for enterprise accounts.

## 4. Required PPE & Lockout/Tagout

- Standard facility PPE only when communications originate from the data floor; office/NOC work requires none.
- Not applicable — no hazardous energy involved in this communication task.

## 5. Regulatory References

- FTC Act §5 (accuracy of service representations to customers); Gramm-Leach-Bliley Safeguards Rule (16 CFR Part 314) where customer financial data is hosted; applicable state breach-notification statutes (e.g., NY SHIELD Act, Cal. Civ. Code §1798.82) for security-incident disclosure; contractual SLA notification terms.
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow

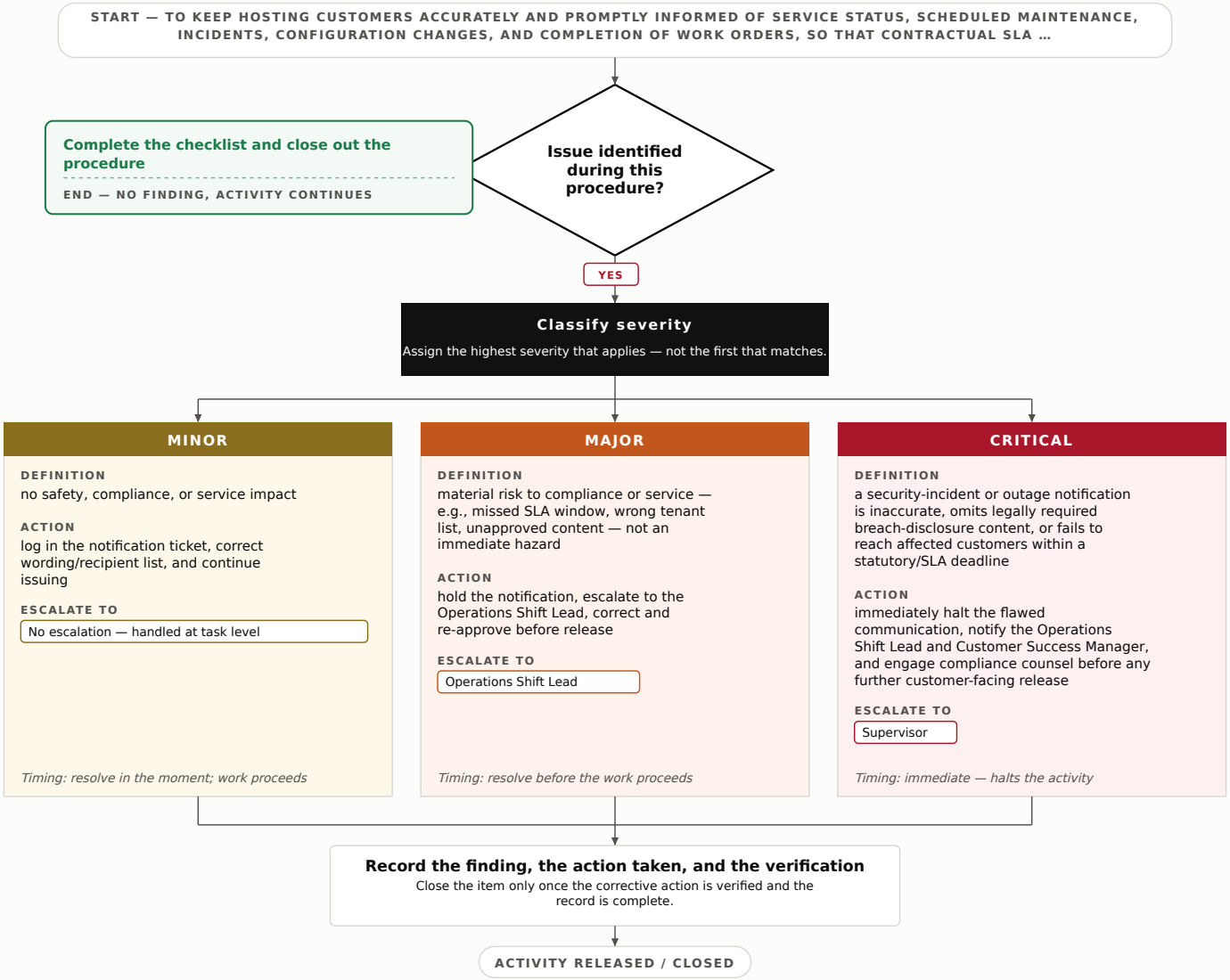

## 7. Step-by-Step Procedure

1. Identify the trigger (scheduled maintenance, monitoring alert, incident ticket, provisioning/migration completion) and confirm the affected hosted services, tenants, and IP ranges from the CMDB.
2. Classify the event severity and determine the SLA notification window applicable to each affected customer tier.
3. Draft the notification using the approved template: event summary, start time, expected impact, affected services, and next-update time — avoid speculation on root cause.
4. Route the draft to the Operations Shift Lead for content and severity approval before release.
5. Issue the approved notification through designated channels (status page, email distribution, customer portal ticket, and enterprise Slack/PagerDuty bridges) within the SLA window.
6. For ongoing incidents, publish interim updates at the committed cadence until service is restored; issue a resolution notice when confirmed stable.
7. For completed work orders (provisioning, migration, hardware turnover to the customer's designated wholesaler-supplied equipment), send a completion notice with verification steps and any customer action required.
8. Record every notification — timestamp, channel, recipients, and content version — in the notification log and attach it to the originating ticket.

## 8. Decision Tree

OD-022 · OPERATIONS · DATA HOSTING

## Decision Tree — Customer Communication & Status Notification




READING THIS TREE

- **No finding** — Activity stands. Complete the checklist and continue.
- **Minor** — Handled in place at task level; no escalation.
- **Major** — Supervisory decision required before the next stage.
- **Critical** — Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- Affected tenant/service list reconciled against the CMDB before issuance.
- Message content and severity approved by the Operations Shift Lead.
- Notification timestamp verified against the applicable SLA window.
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| Trigger source and affected services correctly identified | | |
| Severity classification matches SLA notification tier | | |
| Message uses approved template, no unverified root-cause claims | | |
| Shift Lead approval recorded before release | | |
| Notification issued within SLA window | | |
| Interim update cadence honored for open incidents | | |
| Notification logged and attached to originating ticket | | |

## 11. KPIs

- On-time notification rate within SLA window ≥ 98%
- Notification accuracy (no correction/retraction required) ≥ 99%
- Resolution/completion notice sent within 30 minutes of confirmed restoration ≥ 95%

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# OD-023 — Customer Feedback & Complaint Intake

**Estimated completion time: 15–45 minutes per intake (initial capture, logging, and routing)**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

Establish a consistent method for capturing, logging, and routing customer feedback and complaints about hosting services (uptime, latency, provisioning, billing, data handling) so that every contact is recorded, triaged, and directed to the correct owner without loss or delay.

## 2. Scope

Covers intake of all customer feedback and complaints received via ticketing portal, email, phone, or account manager, and their classification and routing to the responsible team. Excludes root-cause investigation of quality complaints (covered under QC-021) and corrective action (covered under QC-019).

## 3. Responsibilities

- Support Intake Coordinator (OD) — receives, logs, and timestamps each feedback/complaint record; performs initial classification and routing.
- Operations Duty Lead (OD) — validates severity of major/critical items, confirms routing, and owns escalation to on-call engineering.
- Customer Success Manager (OD) — owns customer communication, acknowledgement, and closure confirmation with the account.

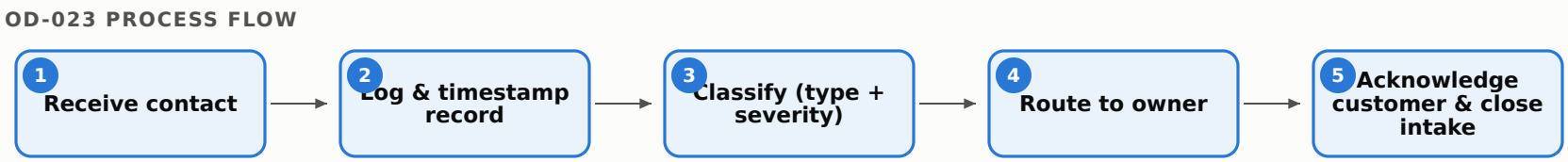
## 4. Required PPE & Lockout/Tagout

- Standard facility PPE (none beyond office/desk environment for intake work; badge access to NOC required).
- Not applicable — no hazardous energy involved.

## 5. Regulatory References

- FTC Act §5 (unfair/deceptive practices — accuracy of complaint handling representations); applicable state data-breach notification statutes where a complaint alleges data exposure; contractual SLA and DPA terms; SOC 2 Common Criteria (complaint/incident logging controls). None additional sector-specific; internal policy applies otherwise.
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow



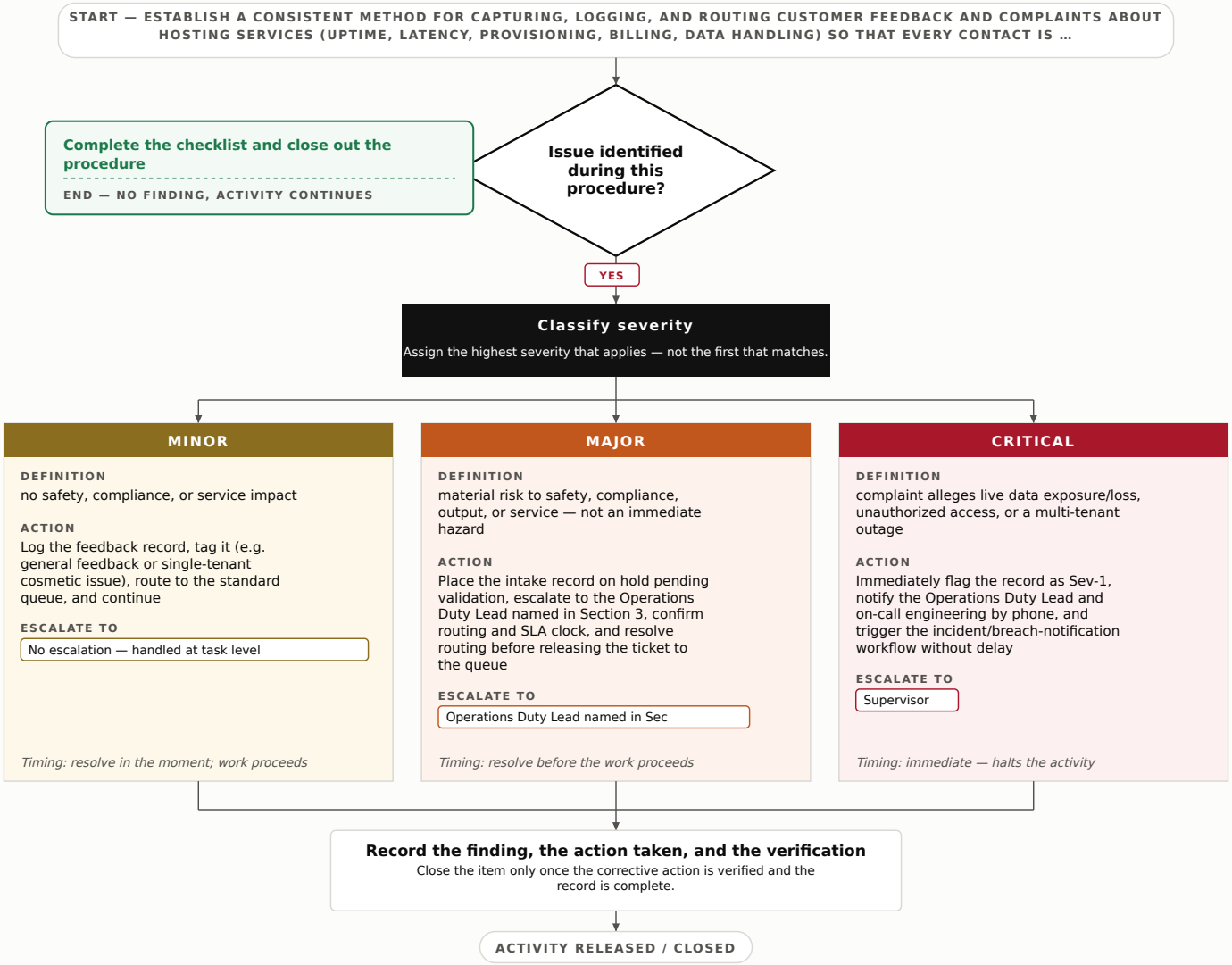

## 7. Step-by-Step Procedure

1. Receive the feedback or complaint through the ticketing portal, monitored inbox, phone queue, or account manager referral.
2. Create a record in the ticketing system, capturing customer/account ID, contact channel, and date/time of receipt.
3. Record the verbatim description, affected service(s), and any environment identifiers (tenant ID, region, service tag).
4. Classify the record by type (uptime/availability, latency/performance, provisioning, billing, data-handling/privacy, general feedback) and by severity per Section 8.
5. Check for related open tickets or known incidents; link duplicates to the parent record rather than creating parallel threads.
6. Route the record to the responsible owner — engineering on-call, billing, or Customer Success — and set the SLA acknowledgement clock.
7. Send the customer an acknowledgement with ticket number and expected next-contact time.
8. Document classification, routing destination, and acknowledgement timestamp in the record before closing the intake stage.

## 8. Decision Tree

OD-023 · OPERATIONS · DATA HOSTING

## Decision Tree — Customer Feedback & Complaint Intake




READING THIS TREE

- **No finding** — Activity stands. Complete the checklist and continue.
- **Minor** — Handled in place at task level; no escalation.
- **Major** — Supervisory decision required before the next stage.
- **Critical** — Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- Every inbound contact has a unique logged record with receipt timestamp.
- Classification (type + severity) is present and matches the description.
- Routing destination and acknowledgement timestamp are recorded before intake closeout.
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| Record created with account ID and channel | | |
| Receipt date/time captured | | |
| Type classification assigned | | |
| Severity classified per Section 8 | | |
| Duplicate/related tickets checked and linked | | |
| Routed to correct owner | | |
| Customer acknowledgement sent with ticket number | | |

## 11. KPIs

- Intake logging completeness — 100% of contacts logged with all required fields.
- Acknowledgement time — ≥95% acknowledged within 1 business hour of receipt.
- Misroute rate — ≤3% of records re-routed after initial assignment.

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# Phase 5 — Oversight & continuity

# OD-024 — Operational Incident Reporting & Response

**Estimated completion time: 30–90 minutes per incident (longer for Critical events involving customer notification)**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

Establish a consistent method for reporting, classifying, and responding to operational incidents and near-misses affecting hosted services — outages, degraded performance, capacity events, failed change windows, and security or availability events — so that service is restored quickly, root cause is captured, and SLA and breach-notification obligations are met.

## 2. Scope

Covers operational and near-miss incidents affecting the availability, performance, or integrity of hosted infrastructure and customer environments in the NOC/data hall, from detection through classification, response, and post-incident review. Excludes personnel safety incident reporting, which is covered under SD-018, and physical equipment breakdown/repair, which is covered under MD-009.

## 3. Responsibilities

- NOC Operations Analyst — detects, opens the incident ticket, performs initial triage, and applies severity classification per this SOP.
- Incident Response Lead — owns response coordination for Major/Critical events, drives restoration, and authorizes customer notifications.
- Operations Manager — reviews closed incidents, chairs post-incident reviews, and approves root-cause corrective actions.

## 4. Required PPE & Lockout/Tagout

- Standard facility PPE for data-hall entry (ESD wrist strap where handling hardware); primarily a workstation/NOC task requiring no additional PPE.
- Not applicable — no hazardous energy involved. Physical remediation requiring energy isolation is handed off per MD-009.

## 5. Regulatory References

- SOC 2 (AICPA Trust Services Criteria — Availability & Security) incident-response controls; NIST SP 800-61 Rev. 2 (Computer Security Incident Handling Guide); applicable breach-notification obligations under state data-breach statutes and, where customer data is in scope, contractual DPA terms. Internal Incident Management Policy applies as the governing baseline.
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow

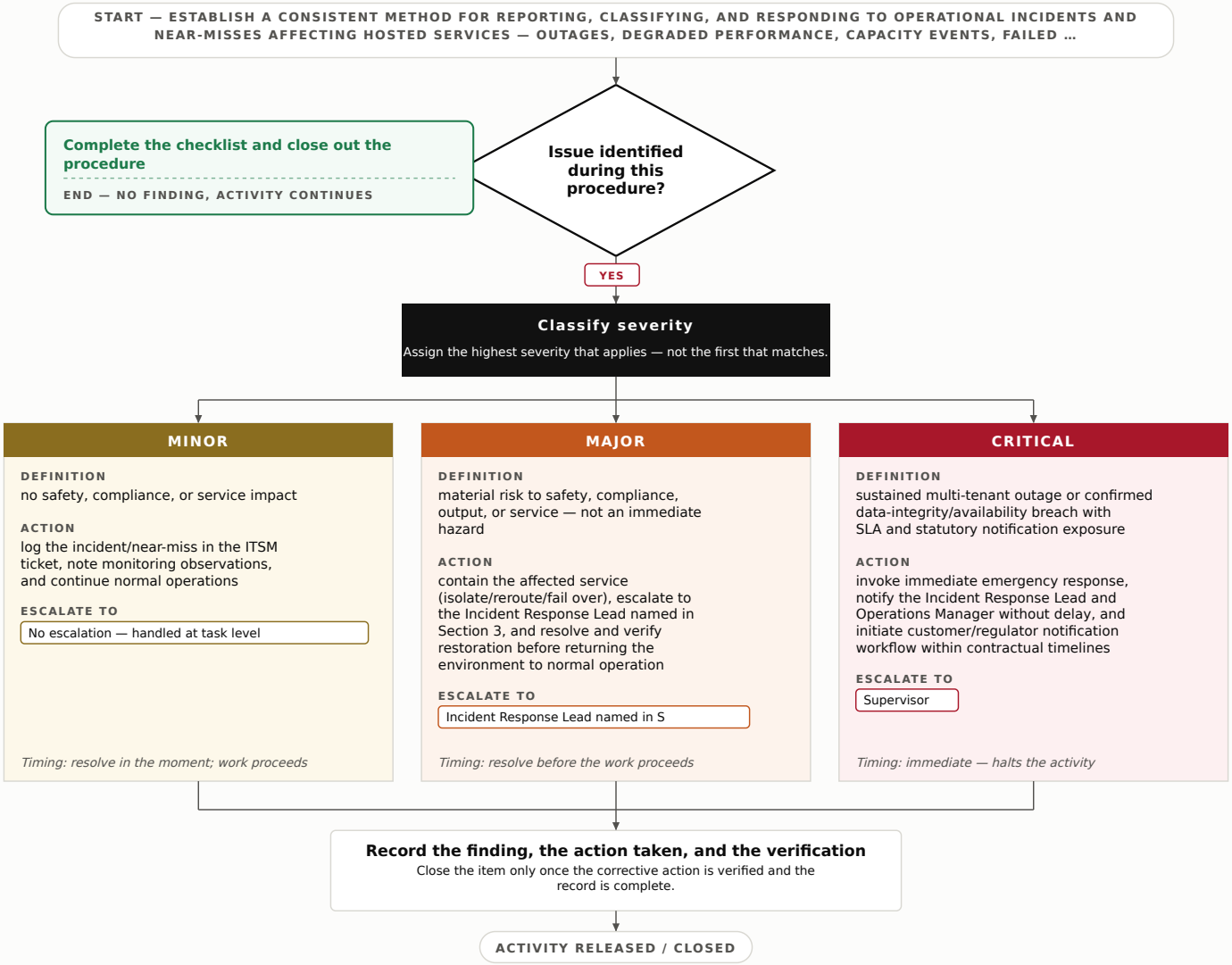

## 7. Step-by-Step Procedure

1. Upon alert, customer report, or observed near-miss, open an incident ticket in the ITSM system and record timestamp, affected service/environment, and detection source.
2. Perform initial triage: confirm scope, identify affected customers/tenants, and check monitoring dashboards for impact (availability, latency, capacity).
3. Classify severity (Minor / Major / Critical) using the Decision Tree in Section 8 and record the classification in the ticket.
4. For Major/Critical, notify the Incident Response Lead and open a coordination bridge; begin containment (isolate affected node, reroute traffic, throttle, or fail over).
5. Execute restoration actions and validate service is healthy against SLA thresholds; confirm with affected customers or account teams as required.
6. Determine whether customer or regulator notification obligations are triggered; if so, route to the Incident Response Lead for authorized notification within contractual/statutory timelines.
7. Conduct root-cause analysis and assign corrective/preventive actions with owners and due dates.
8. Close the ticket with full timeline, classification, resolution, and RCA attached; log near-misses even where no service impact occurred.

## 8. Decision Tree

OD-024 · OPERATIONS · DATA HOSTING

## Decision Tree — Operational Incident Reporting & Response




**READING THIS TREE**

- **No finding** — Activity stands. Complete the checklist and continue.
- **Minor** — Handled in place at task level; no escalation.
- **Major** — Supervisory decision required before the next stage.
- **Critical** — Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- Every incident and near-miss has a ticket with timestamp, severity, and affected-service fields completed.
- Major/Critical incidents have a documented response timeline and confirmed service restoration against SLA.
- Notification decisions (customer/regulator) are recorded with rationale and, where triggered, dispatch time.
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| Incident ticket opened with detection source and timestamp | | |
| Affected services/tenants identified and documented | | |
| Severity classified per Decision Tree | | |
| Containment/restoration actions logged with timestamps | | |
| Notification obligation assessed and recorded | | |
| Root-cause analysis and corrective actions assigned | | |
| Ticket closed with complete timeline and RCA attached | | |

## 11. KPIs

- Mean time to acknowledge (MTTA) for Major/Critical incidents ≤ 15 minutes.
- Incidents classified with correct severity on first pass ≥ 95%.
- Post-incident reviews completed for 100% of Critical incidents within 5 business days.

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# OD-025 — Emergency & Business Continuity Readiness Check

**Estimated completion time: 3–5 hours (quarterly review cycle)**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

This procedure verifies that the data hosting operation can detect a disruption, sustain critical customer workloads, and resume normal service within committed recovery objectives. It confirms that continuity documentation, contact chains, and failover readiness records are current and actionable.

## 2. Scope

Covers the readiness verification of business continuity and disaster-recovery documentation, contact rosters, failover-site status, and restoration checkpoints for hosted production environments in Operations. Excludes emergency drills and live response execution, which are covered under SD-015 and SD-016, and backup power systems, which are covered under ED-027.

## 3. Responsibilities

- Operations Continuity Lead — owns the BC/DR plan, runs this readiness check, and closes findings.
- Data Center Operations Manager — validates failover-site status, RTO/RPO commitments, and escalation authority.
- NOC Shift Supervisor — confirms monitoring alerts, contact roster accuracy, and on-call coverage for continuity events.

## 4. Required PPE & Lockout/Tagout

- Standard facility PPE for any walk-through of the data hall (ESD strap when near live racks; hearing awareness in hot/cold aisles).
- Not applicable — this is a documentation and readiness-verification task involving no hazardous energy or physical isolation.

## 5. Regulatory References

- SOC 2 (AICPA TSC — Availability criteria A1.2, A1.3 for recovery and continuity)
- ISO 22301:2019 (Business Continuity Management Systems)
- ISO/IEC 27001:2022 Annex A.5.29–A.5.30 (information security during disruption / ICT readiness for continuity)
- NIST SP 800-34 Rev. 1 (Contingency Planning Guide for Federal Information Systems) — reference framework
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow


## 7. Step-by-Step Procedure

1. Retrieve the current, version-controlled BC/DR plan and confirm the revision date is within the last review interval (≤ 12 months).
2. Verify the critical-service inventory lists all in-scope hosted workloads with assigned RTO and RPO values and current customer SLA mappings.
3. Confirm the emergency contact roster and escalation chain (Continuity Lead, Ops Manager, NOC, key vendors) — validate every phone/email entry against HR and vendor records.
4. Verify failover-site status: confirm the DR site or region is reachable, replication is current, and last successful failover test result is on file (execution itself owned by SD-016).
5. Confirm restoration checkpoints exist for each tier — data restore order, dependency map, and last successful restore-verification timestamp; confirm backup power hand-off is referenced per ED-027.
6. Review monitoring/alert configuration with NOC to confirm disruption-detection thresholds route to the correct on-call roles.
7. Reconcile any gaps found against prior open findings; classify per the Decision Tree.
8. Record verification results, sign-offs, and corrective-action assignments in the continuity readiness log.

## 8. Decision Tree

OD-025 · OPERATIONS · DATA HOSTING

## Decision Tree — Emergency & Business Continuity Readiness Check

START — THIS PROCEDURE VERIFIES THAT THE DATA HOSTING OPERATION CAN DETECT A DISRUPTION, SUSTAIN CRITICAL CUSTOMER WORKLOADS, AND RESUME NORMAL SERVICE WITHIN COMMITTED RECOVERY OBJECTIVES. IT CONFIRMS …

**Issue identified during this procedure?**

NO → **Complete the checklist and close out the procedure**

END — NO FINDING, ACTIVITY CONTINUES

YES

**Classify severity**

Assign the highest severity that applies — not the first that matches.

### MINOR

DEFINITION

no safety, compliance, or service impact

ACTION

Log in the continuity readiness log with an owner and due date; continue the review

ESCALATE TO

No escalation — handled at task level

*Timing: resolve in the moment; work proceeds*

### MAJOR

DEFINITION

material risk to safety, compliance, output, or service — not an immediate hazard

ACTION

Hold the affected continuity record from customer-facing release, escalate to the Data Center Operations Manager, and resolve before the readiness check is signed off

ESCALATE TO

Data Center Operations Manager

*Timing: resolve before the work proceeds*

### CRITICAL

DEFINITION

a workload with committed RTO/RPO has no verified, current failover or restoration path, meaning a disruption could cause unrecoverable customer data loss or SLA breach

ACTION

Immediately notify the Operations Continuity Lead and Data Center Operations Manager, open a priority remediation ticket, and suspend the readiness attestation until a verified recovery path exists

ESCALATE TO

Supervisor

*Timing: immediate — halts the activity*

**Record the finding, the action taken, and the verification**

Close the item only once the corrective action is verified and the record is complete.

ACTIVITY RELEASED / CLOSED

READING THIS TREE

- **No finding** — Activity stands. Complete the checklist and continue.
- **Minor** — Handled in place at task level; no escalation.
- **Major** — Supervisory decision required before the next stage.
- **Critical** — Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- BC/DR plan revision date current and version-controlled.
- Every in-scope workload has verified RTO/RPO and a mapped restoration checkpoint.
- Contact roster and escalation chain reconciled against HR/vendor records within this cycle.
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| BC/DR plan is current (≤ 12 months) and version-controlled | | |
| Critical-service inventory lists RTO/RPO for all in-scope workloads | | |
| Emergency contact roster and escalation chain verified | | |
| Failover-site reachable with current replication status on file | | |
| Restoration/data-recovery checkpoints documented per tier | | |
| Monitoring alerts route to correct on-call roles | | |
| Prior open findings reconciled and dispositioned | | |

## 11. KPIs

- BC/DR readiness reviews completed on schedule: 100% per quarter.
- Workloads with a verified current recovery path: ≥ 99%.
- Open Critical continuity findings at sign-off: 0.

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# OD-026 — Regulatory, License & Permit Currency Verification

**Estimated completion time: 3–5 hours per verification cycle (quarterly)**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

This procedure confirms that all operating licenses, permits, and registrations required to run the Data Hosting facility — business operating licenses, generator/air permits, data-protection registrations, and applicable framework certifications — remain current, valid, and correctly scoped so that colocation and hosting services continue without lapse or regulatory exposure.

## 2. Scope

Covers scheduled and event-triggered verification of the facility's regulatory currency register: municipal business licenses, environmental/standby-generator permits, data-privacy registrations (e.g., state privacy filings, EU representative registrations), and third-party attestations (SOC 2, ISO/IEC 27001, PCI DSS). Excludes safety regulatory compliance, which is covered under SD-028, and permit-to-work authorization, which is covered under MD-007.

## 3. Responsibilities

- Operations Compliance Lead — owns the regulatory currency register, initiates each verification cycle, and approves close-out.
- Facilities Operations Manager — supplies status of site/environmental permits (standby generator air permits, fire/occupancy) and coordinates renewals.
- Records & Documentation Coordinator — files evidence, tracks expiry dates, and maintains the audit trail in the compliance repository.

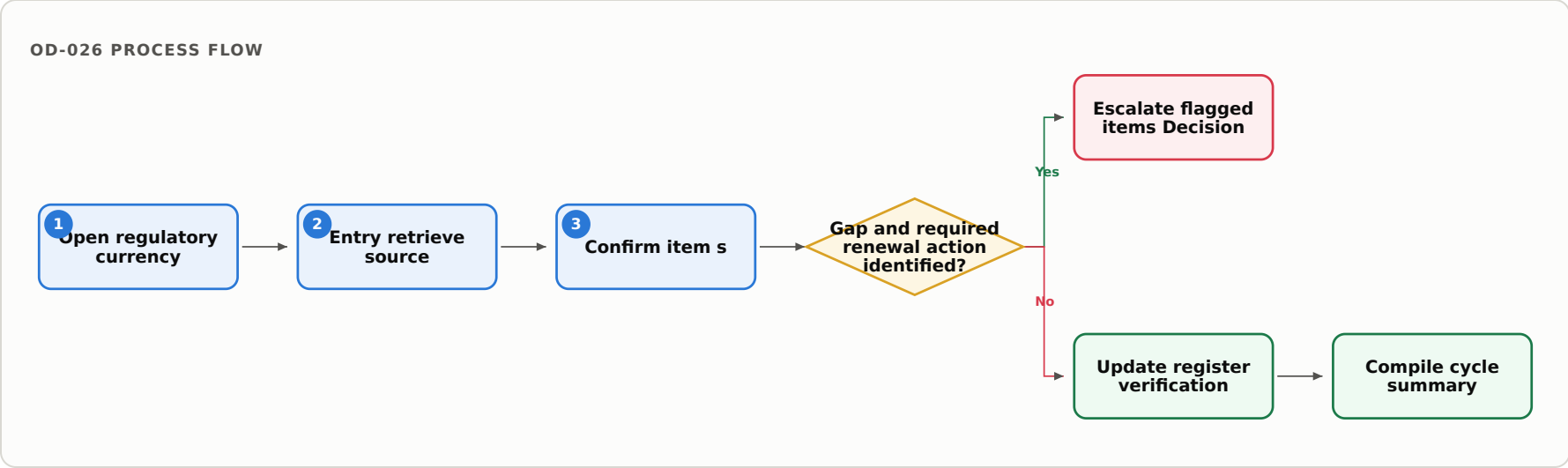
## 4. Required PPE & Lockout/Tagout

- Standard facility PPE (none specific — administrative task performed in office/NOC area).
- Not applicable — no hazardous energy involved.

## 5. Regulatory References

- SOC 2 (AICPA TSC), ISO/IEC 27001:2022, PCI DSS v4.0 (where card data is processed), and applicable state data-privacy statutes (e.g., CCPA/CPRA); local business-license and environmental air-permit rules governing standby generators (EPA 40 CFR Part 60 Subpart JJJJ / IIII, as applicable to facility engines).
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow



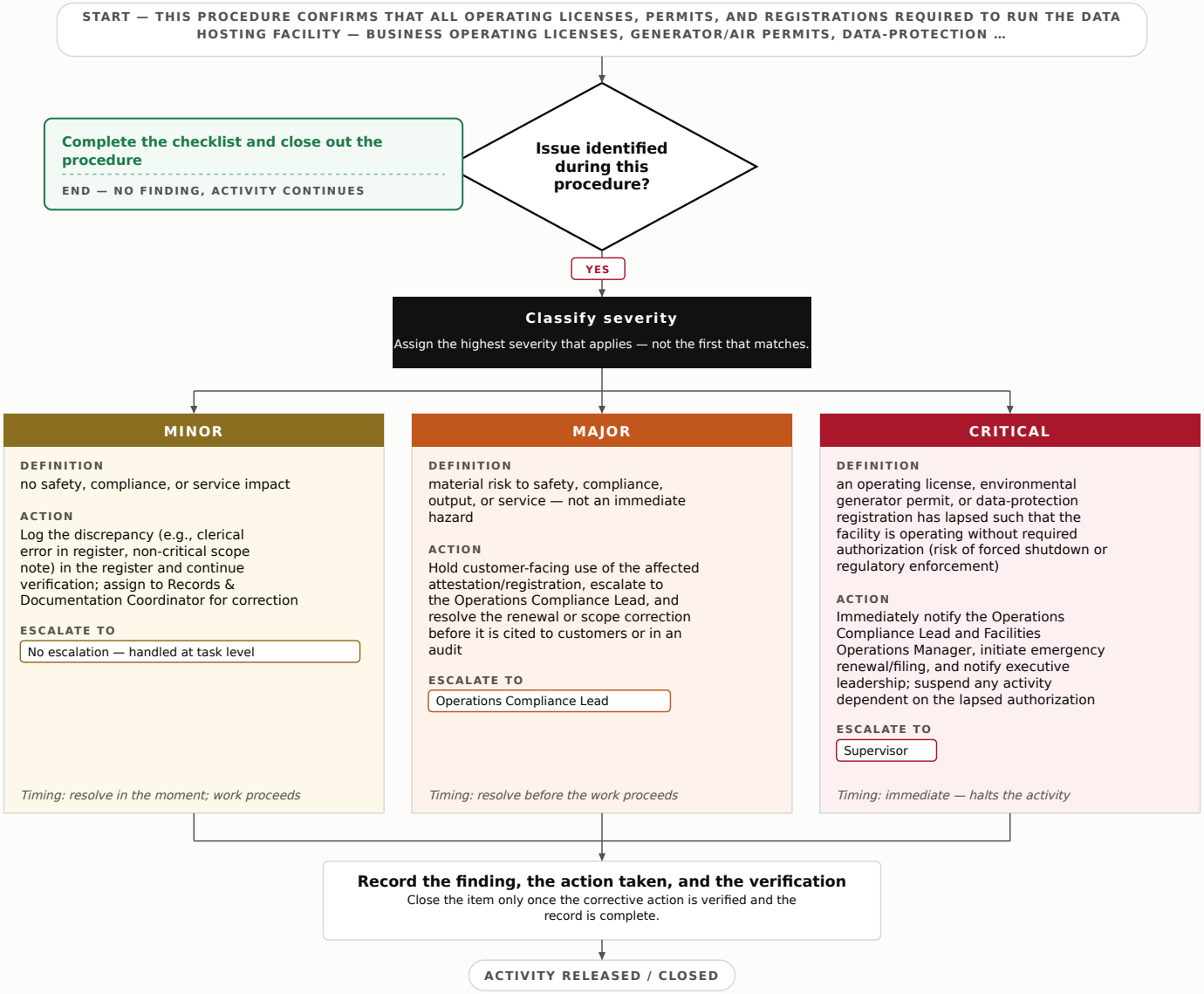

## 7. Step-by-Step Procedure

1. Open the regulatory currency register and confirm every required license, permit, and registration for the facility is listed with issuing authority, number, scope, and expiry date.
2. For each entry, retrieve the source document (certificate, permit, filing receipt) and verify it against the issuing authority's public record or renewal portal where available.
3. Confirm each item's scope still matches current operations (facility square footage, generator count/capacity, data-processing activities, customer data categories).
4. Verify third-party attestations (SOC 2 report period, ISO/IEC 27001 certificate, PCI DSS AOC) are within their valid window and cover the in-scope services.
5. Identify any item expired, expiring within 90 days, or scope-mismatched; record the gap and required renewal action.
6. Escalate flagged items per the Decision Tree and assign an owner and target date for renewal.
7. Update the register with verification date, status, and evidence links; attach screenshots or confirmation numbers.
8. Compile the cycle summary, obtain Operations Compliance Lead sign-off, and archive per retention policy.

## 8. Decision Tree

OD-026 · OPERATIONS · DATA HOSTING

## Decision Tree — Regulatory, License & Permit Currency Verification




READING THIS TREE

- **No finding** — Activity stands. Complete the checklist and continue.
- **Minor** — Handled in place at task level; no escalation.
- **Major** — Supervisory decision required before the next stage.
- **Critical** — Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- Every register entry has verifiable source evidence dated within the current cycle.
- All expiry dates cross-checked against issuing-authority records, not just internal copies.
- Every flagged item has an assigned owner and target renewal date.
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| Business/operating license current and on file | | |
| Standby-generator/environmental air permit current and scope-matched | | |
| SOC 2 report period valid and covers in-scope services | | |
| ISO/IEC 27001 certificate within valid window | | |
| PCI DSS AOC current (if card data processed) | | |
| Data-privacy registrations/filings current | | |
| Register updated with verification date and evidence links | | |

## 11. KPIs

- License/permit currency rate: 100% of required items valid at cycle close.
- Renewal lead time: no item allowed within 30 days of expiry unrenewed (target ≥90-day advance flag).
- Verification cycle completion: quarterly cycle closed within 5 business days of start.

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# OD-027 — Operational Risk Review

**Estimated completion time: 4–6 hours per review cycle (quarterly)**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

This procedure establishes a recurring review of operational risks and their mitigating controls across the data hosting environment — power, cooling, network, storage, and service continuity — so that risk exposure to hosted customer workloads is identified, scored, and tracked to closure before it degrades availability or SLA commitments.

## 2. Scope

Covers periodic review of operational risk registers, control effectiveness, and residual-risk acceptance for colocation and managed-hosting operations. Excludes safety hazard/risk assessment, which is covered under SD-004, and quality preventive action, which is covered under QC-020.

## 3. Responsibilities

- Operations Risk Lead — owns the risk register, facilitates the review cycle, and assigns risk owners and treatment actions.
- Data Center Operations Manager — validates control effectiveness for facility systems (power, cooling, physical access) and approves residual-risk acceptance.
- Infrastructure/NOC Engineer — supplies operational data (uptime, capacity, incident trends) and confirms technical control status for compute, storage, and network layers.

## 4. Required PPE & Lockout/Tagout

- Standard facility PPE only when the review requires a walkdown of the data floor (hearing protection, ESD wrist strap in equipment zones).
- Not applicable — no hazardous energy involved in the review activity itself; any physical inspection is observational only.

## 5. Regulatory References

- SOC 2 (AICPA TSC) Availability & Confidentiality criteria; ISO/IEC 27001:2022 Clause 6.1 and Annex A operational controls; NIST SP 800-30 (risk assessment methodology); ISO 22301 (business continuity) where BC risks are in scope. Internal policy: Operational Risk Management Standard applies where no sector-specific mandate governs.
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow

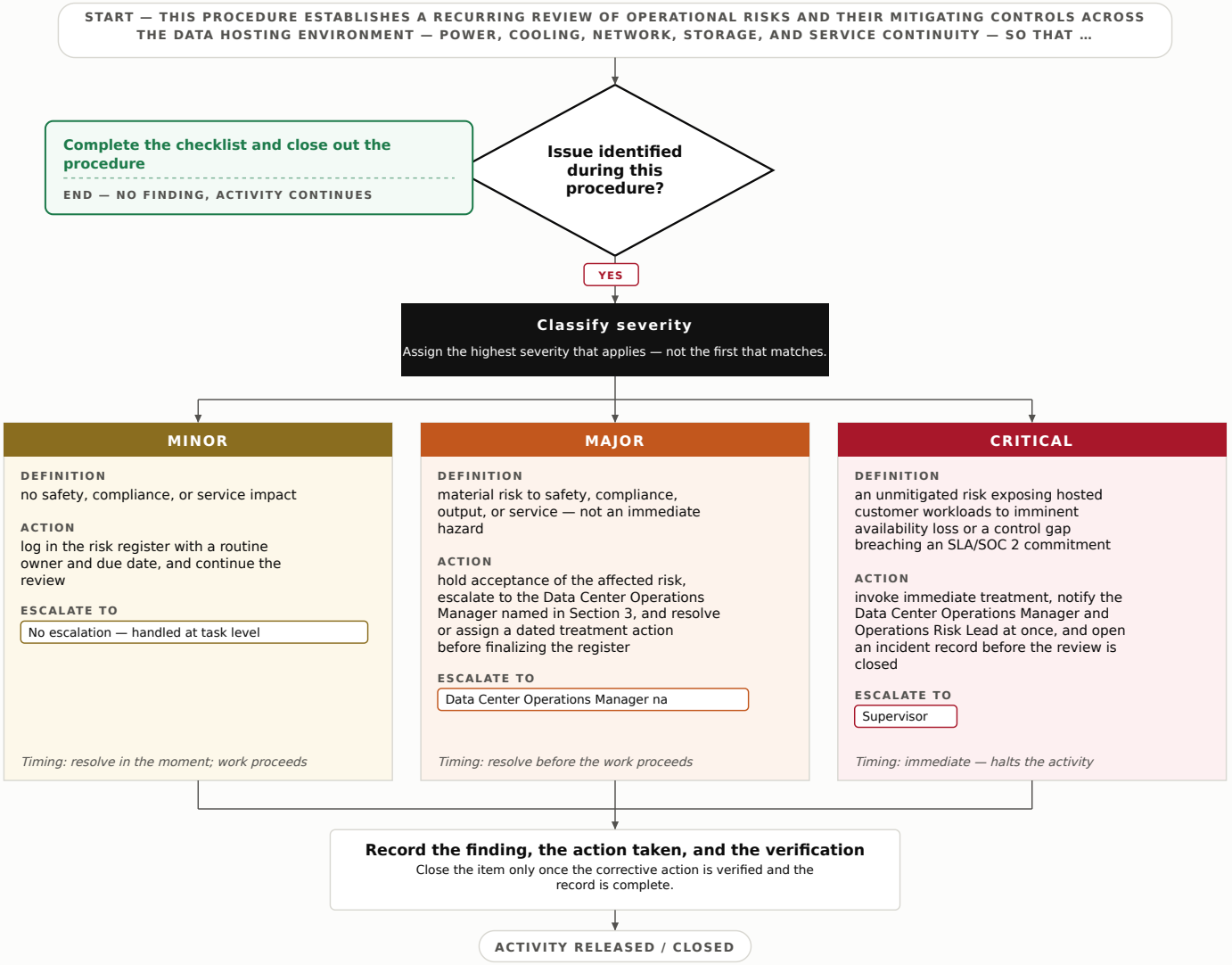

## 7. Step-by-Step Procedure

1. Retrieve the current operational risk register and confirm the review scope (power/UPS, cooling/CRAC, network, storage arrays, physical access, capacity, vendor dependencies).
2. Collect operational evidence since last review: uptime/SLA reports, incident and change records, capacity-utilization trends, environmental alarms, and DR test results.
3. Re-evaluate each existing risk using the likelihood × impact matrix (NIST SP 800-30 basis); add newly identified operational risks surfaced from incidents or changes.
4. Assess the effectiveness of each mitigating control (e.g., N+1 power redundancy, dual-path network, monitored access control) and flag any degraded, missing, or untested control.
5. Assign or update a risk owner and treatment action (accept, mitigate, transfer) with a due date for every risk scored Major or above.
6. Confirm residual-risk levels and obtain Data Center Operations Manager sign-off for any accepted residual risk above the defined threshold.
7. Verify no open item overlaps QC-020 preventive-action or SD-004 safety scope; hand off by reference where applicable.
8. Publish the updated register, distribute the review summary to stakeholders, and record the review in the operational records log with the next cycle date.

## 8. Decision Tree

OD-027 · OPERATIONS · DATA HOSTING

## Decision Tree — Operational Risk Review




READING THIS TREE

- **No finding** — Activity stands. Complete the checklist and continue.
- **Minor** — Handled in place at task level; no escalation.
- **Major** — Supervisory decision required before the next stage.
- **Critical** — Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- Every risk in scope has a current score, owner, and treatment status.
- Control-effectiveness assessment references verifiable evidence (report, test, or log), not assertion.
- Residual-risk acceptances above threshold carry documented Operations Manager sign-off.
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| Risk register reflects current review date and scope | | |
| Operational evidence (uptime, incidents, capacity) collected | | |
| All existing risks re-scored via likelihood × impact matrix | | |
| Control effectiveness assessed for power, cooling, network, storage | | |
| Treatment actions assigned with owners and due dates | | |
| Residual-risk acceptances approved and documented | | |
| Review recorded and next cycle scheduled | | |

## 11. KPIs

- Risk register review completed on schedule — 100% of quarterly cycles.
- Major/Critical risks with an assigned dated treatment action — 100%.
- Overdue risk treatment actions at cycle close — ≤ 5%.

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# Phase 6 — Performance, records & close

# OD-028 — Operational KPI Review

**Estimated completion time: 2–4 hours per review cycle**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

Establish a repeatable process for reviewing facility-wide operational performance — uptime, power/cooling efficiency, incident response, and capacity utilization — against defined targets so the Operations team can detect drift, protect customer SLAs, and drive corrective action at a Data Hosting facility.

## 2. Scope

Covers the periodic review of operations-level KPIs (availability, PUE, environmental setpoints, ticket/incident throughput, capacity headroom) across the hosting floor and supporting infrastructure. Excludes department-specific KPI reviews for maintenance, quality control, and service delivery, which are covered under MD-030, QC-030, and SD-030 respectively; this procedure addresses operations measures only.

## 3. Responsibilities

- Operations Manager — owns the review, approves targets, signs off on corrective actions and escalations.
- Data Center Operations Lead — compiles KPI data from DCIM/monitoring systems, prepares the review pack, tracks action items.
- NOC Shift Supervisor — validates incident and availability data against shift logs and confirms real-time accuracy of feeds.

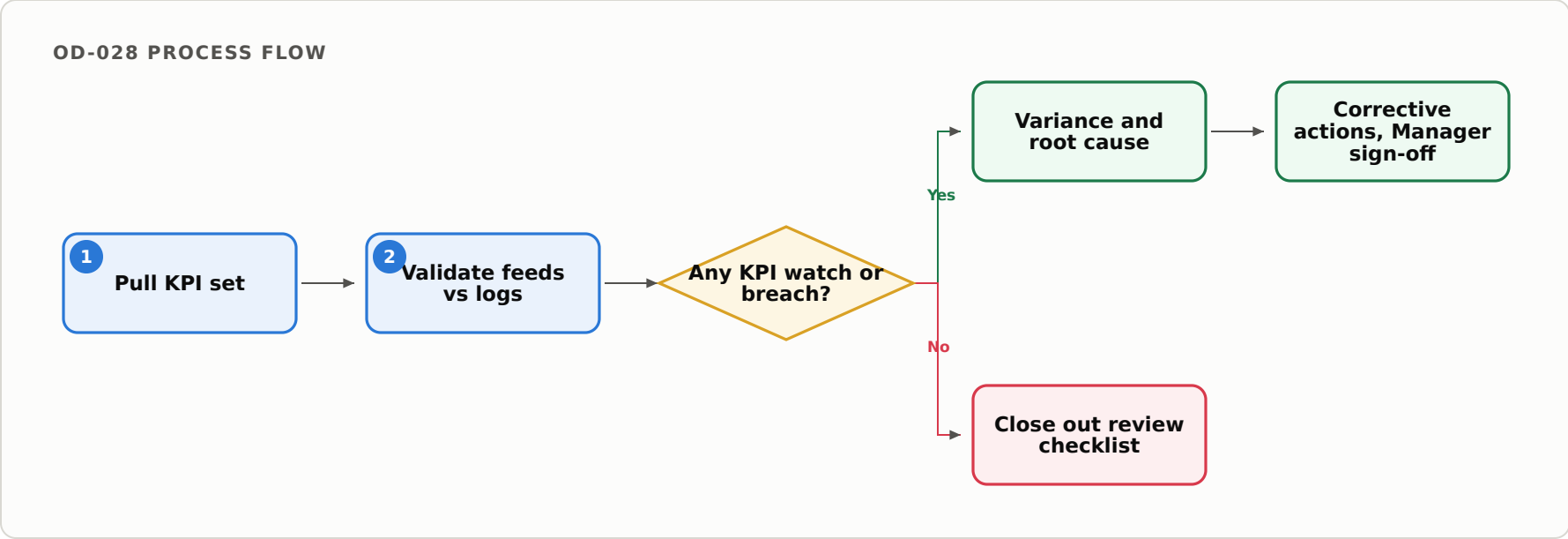
## 4. Required PPE & Lockout/Tagout

- Standard facility PPE only for any incidental floor walk (ESD wrist strap if touching racks); office/desk task otherwise.
- Not applicable — no hazardous energy involved; this is a data review task.

## 5. Regulatory References

- None sector-specific to KPI review; internal Operations Policy and customer SLA contracts apply. Related frameworks that may govern the underlying metrics: SOC 2 (AICPA Trust Services Criteria — Availability), ISO/IEC 27001, and ASHRAE TC 9.9 thermal guidelines for environmental setpoints.
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow



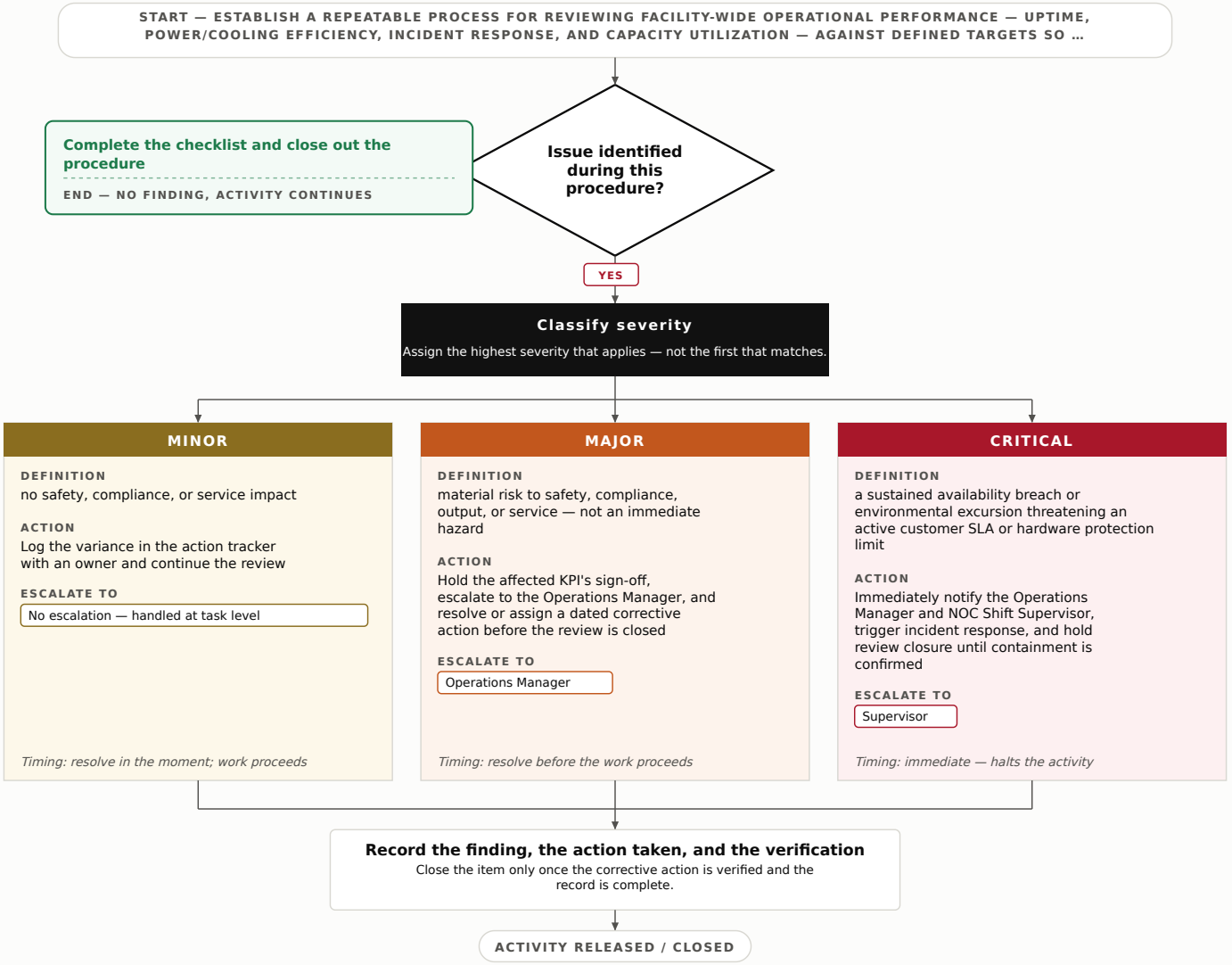

## 7. Step-by-Step Procedure

1. Confirm the review period and pull the current operations KPI set from DCIM, BMS, and the NOC ticketing system (availability %, PUE, inlet temp/humidity compliance, MTTR, capacity utilization).
2. Cross-check each data feed against NOC shift logs and BMS records to confirm data integrity before analysis; flag any gaps or sensor faults.
3. Compare each KPI against its defined target and control threshold; mark each as on-target, watch, or breach.
4. For any watch or breach metric, perform variance analysis — identify trend direction, contributing events, and affected customers/SLAs.
5. Determine root cause for breaches and draft corrective or preventive actions with owners and due dates.
6. Confirm any hand-offs to department-specific reviews (MD-030, QC-030, SD-030) are logged without duplicating their analysis.
7. Present findings to the Operations Manager, agree on actions, and classify any issues per the Decision Tree.
8. Document the completed review pack, action log, and sign-off in the Operations records repository with the review date and period.

## 8. Decision Tree

OD-028 · OPERATIONS · DATA HOSTING

## Decision Tree — Operational KPI Review




### READING THIS TREE

**No finding**
Activity stands. Complete the checklist and continue.

**Minor**
Handled in place at task level; no escalation.

**Major**
Supervisory decision required before the next stage.

**Critical**
Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- All KPI feeds validated against source logs before analysis
- Every breach has a documented root cause and dated corrective action
- Hand-offs to MD-030/QC-030/SD-030 acknowledged, not duplicated
- Zero unresolved Critical findings

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| Review period and KPI set confirmed | | |
| Data feeds validated against NOC/BMS logs | | |
| Each KPI compared to defined target/threshold | | |
| Variance and root-cause analysis complete for breaches | | |
| Corrective actions assigned with owners and due dates | | |
| SLA-impacting metrics flagged and escalated as needed | | |
| Review pack documented and signed off | | |

## 11. KPIs

- Facility availability (uptime) ≥ 99.982% per review period
- Power Usage Effectiveness (PUE) ≤ 1.5 rolling average
- Mean Time To Resolve (MTTR) for operations incidents ≤ 4 hours

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# OD-029 — Operational Records Retention & Documentation Audit

**Estimated completion time: 4–6 hours per quarterly audit cycle**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

This procedure ensures that operational records — data center facility logs, change-management tickets, access logs, capacity and uptime reports, and maintenance records — are complete, accurate, and retained for the required periods so the Data Hosting operation can demonstrate compliance during customer and SOC 2 audits.

## 2. Scope

Covers the periodic verification and retention audit of Operations records (facility environmental logs, change tickets, incident records, backup/restore verification logs, and equipment lifecycle records) held in the DCIM and ticketing systems. Excludes quality records (see QC-029), safety records (see SD-029), and HR records (see HR-029).

## 3. Responsibilities

- Operations Records Custodian — executes the audit, samples record sets, and logs findings in the audit register.
- Data Center Operations Manager — approves retention schedules, reviews findings, and authorizes remediation or disposition.
- Compliance Coordinator — confirms retention periods against customer contracts and applicable standards, and owns escalation of Critical findings.

## 4. Required PPE & Lockout/Tagout

- Standard facility PPE when accessing the data hall for physical log verification (ESD-safe footwear, badge access); office-standard for records review.
- Not applicable — no hazardous energy involved; this is a records and documentation task.

## 5. Regulatory References

- SOC 2 (AICPA TSC) audit-trail and record-retention criteria; ISO/IEC 27001 Annex A.12.4 (logging and monitoring) and A.18.1 (records management); Sarbanes-Oxley §802 and applicable customer contractual/data-residency retention terms.
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow

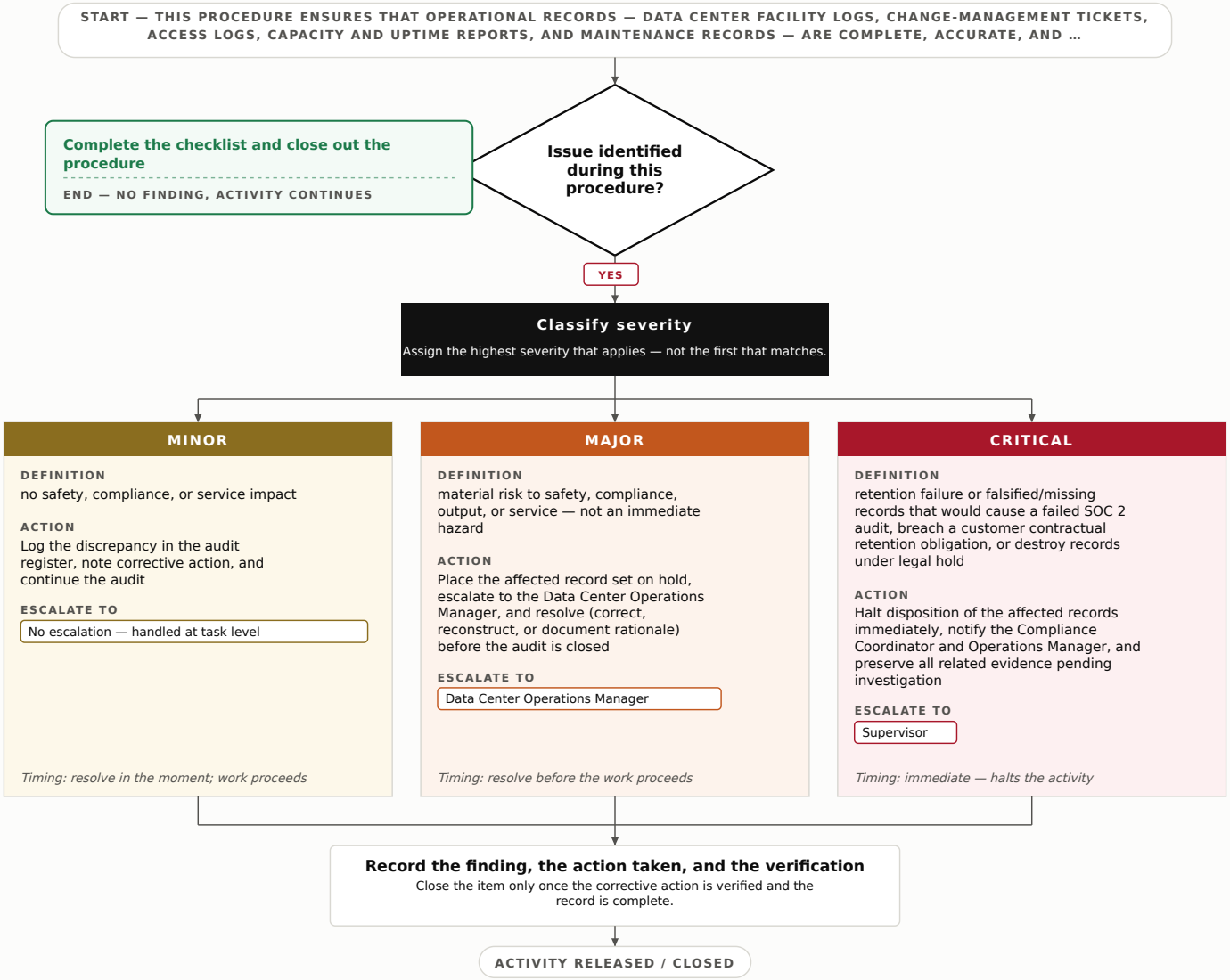

## 7. Step-by-Step Procedure

1. Retrieve the current operational records inventory and the approved retention schedule from the Compliance Coordinator.
2. Identify the record categories in scope for this cycle (facility environmental logs, change tickets, incident logs, backup verification records, equipment lifecycle records).
3. Pull a representative sample from the DCIM and ticketing systems, covering the full audit period, no fewer than 10% of records per category.
4. Verify each sampled record is complete — required fields populated, timestamps present, approvals attached, and no gaps in continuous logs.
5. Verify accuracy by cross-checking a subset against source events (e.g., change ticket against actual change window, incident record against monitoring alert).
6. Confirm each record is retained for its required period and that expired records are dispositioned per schedule (retained, archived, or securely destroyed).
7. Classify and log any discrepancies in the audit register using the Section 8 decision tree.
8. Record audit results, remediation actions, and disposition decisions in the quarterly audit report and route to the Operations Manager for sign-off.

## 8. Decision Tree

OD-029 · OPERATIONS · DATA HOSTING

## Decision Tree — Operational Records Retention & Documentation Audit




READING THIS TREE

- **No finding** — Activity stands. Complete the checklist and continue.
- **Minor** — Handled in place at task level; no escalation.
- **Major** — Supervisory decision required before the next stage.
- **Critical** — Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- Retention schedule confirmed current and matched to sampled categories.
- Sample size and coverage meet the minimum threshold for the audit period.
- All Major findings have documented remediation and Manager sign-off.
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| Record inventory matches approved retention schedule | | |
| Facility environmental & DCIM logs complete, no gaps | | |
| Change tickets carry required approvals and timestamps | | |
| Incident and backup-verification records reconcile to source events | | |
| Expired records dispositioned per schedule | | |
| Records under legal hold flagged and preserved | | |
| Audit findings logged and remediation assigned | | |

## 11. KPIs

- Record completeness rate ≥ 99% of sampled records.
- Retention compliance rate = 100% (no records disposed before required period).
- Audit findings remediated within 15 business days ≥ 95%.

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |

# OD-030 — End-of-Shift / End-of-Day Operations Closeout

**Estimated completion time: 45–90 minutes**

> Provided for general informational and operational purposes as part of the Data Hosting archetype library. Does not constitute a certified safety program. Verify all regulatory references and equipment-specific tolerances with a qualified engineer or safety professional before implementation.

## 1. Purpose

This procedure closes the operating period at a data hosting facility by securing the floor and NOC, confirming backup and monitoring continuity, reconciling ticket and change activity, and documenting the state of the environment so the next period begins from a known-good baseline.

## 2. Scope

Covers end-of-shift and end-of-day closeout of the NOC/operations floor, including environmental checks, backup/replication verification, ticket reconciliation, physical and logical securing, and closeout documentation. Excludes opening procedures (see OD-001) and the shift handover briefing itself (see OD-002); this module prepares the record that feeds that handover but does not author it.

## 3. Responsibilities

- Shift Operations Lead (NOC) — owns the closeout, verifies backup/replication status, signs the closeout record.
- Data Center Technician — performs physical floor walk, environmental and rack-security checks, and console lockouts.
- Operations Supervisor — reviews unresolved Major/Critical findings and authorizes closeout when exceptions exist.

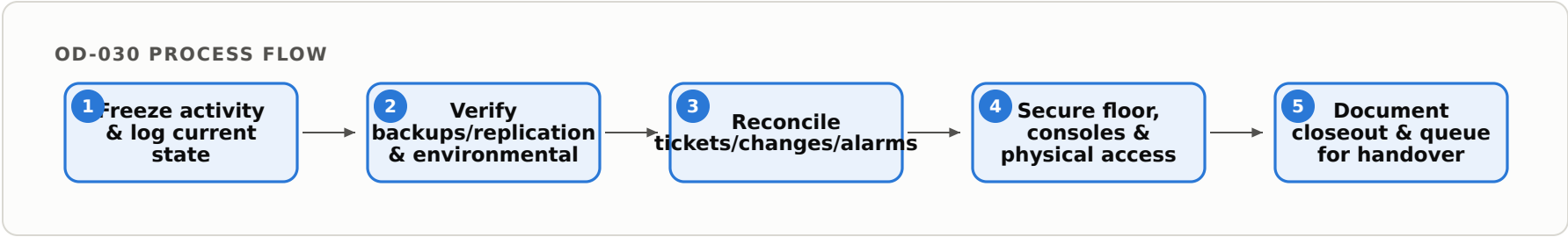
## 4. Required PPE & Lockout/Tagout

- Standard facility PPE: ESD wrist strap when contacting rack hardware; badge/ID visible at all times.
- Lockout/Tagout: Not applicable — no hazardous energy is de-energized in this task; do not open PDU or UPS panels during closeout.

## 5. Regulatory References

- SOC 2 (AICPA TSC) control activities for availability and confidentiality; ISO/IEC 27001 Annex A logging and operations controls; PCI DSS Req. 10 (logging/monitoring) and Req. 9 (physical access) where cardholder-data hosting applies; NIST SP 800-53 AU/CP control families as internal-policy basis.
- Note: confirm applicability of sector-specific standards and any state-plan equivalents for this facility before customer-facing release.

## 6. Process Flow



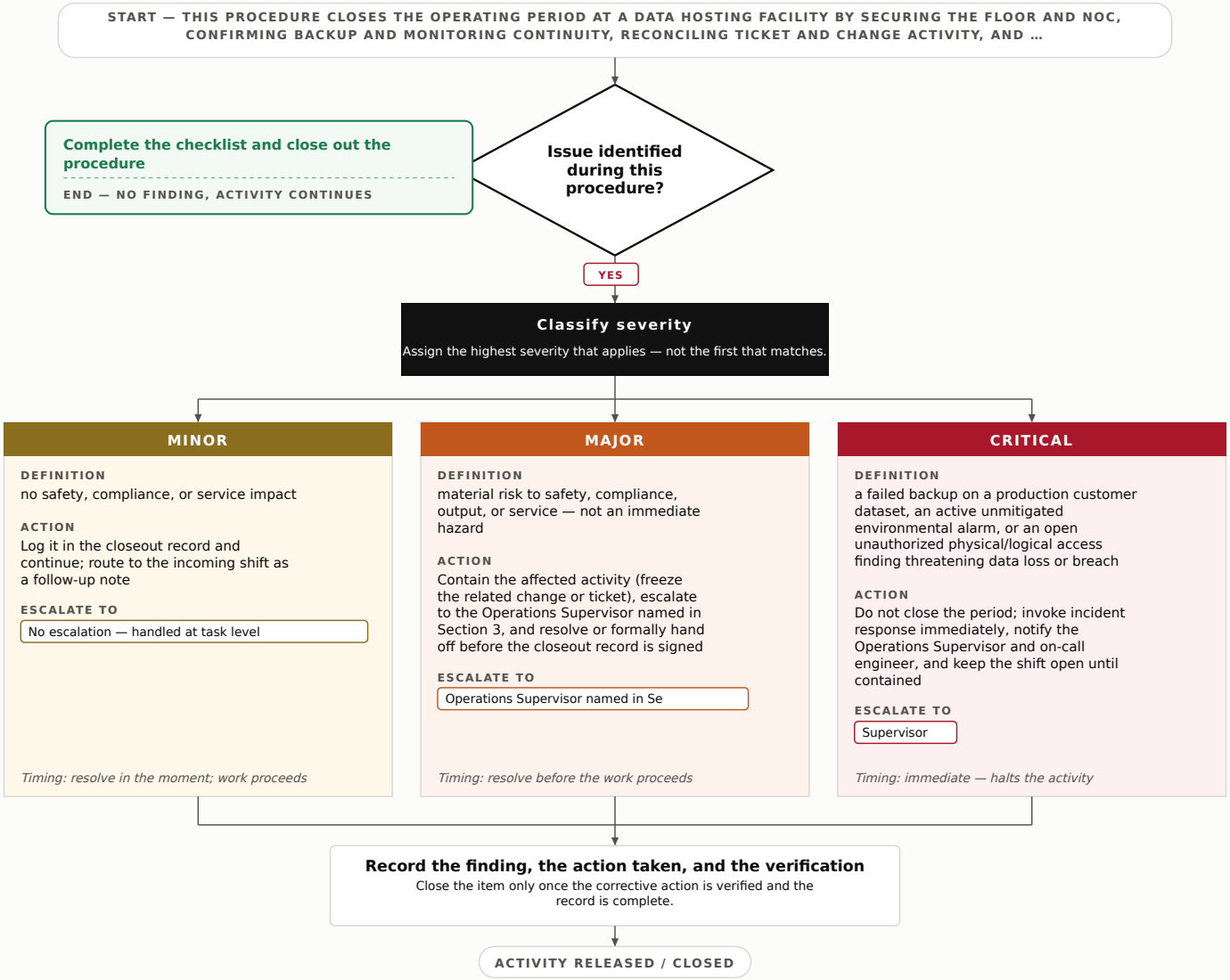

## 7. Step-by-Step Procedure

1. Announce closeout window in the NOC channel and confirm no active customer-impacting change or maintenance is mid-execution; if one is, note owner and expected completion.
2. Review the monitoring dashboards (temperature/humidity, power draw, network utilization) and confirm all environmental readings are within threshold; capture any active or acknowledged alarms.
3. Verify scheduled backup and replication jobs for the period completed successfully; record any failed/partial jobs with job ID and affected system.
4. Reconcile the ticket queue: confirm all resolved tickets are closed with notes, open tickets have current status, and any escalations are assigned to the incoming shift.
5. Perform the physical floor walk — verify rack doors secured, cage/cabinet locks engaged, no unattended tools or media, and spares/inbound hardware from suppliers logged and stored.
6. Secure logical access — log out or lock shared consoles and KVM sessions, confirm privileged sessions are terminated, and verify access logs are being written.
7. Confirm no pending outbound service turnover (customer environment provisioning or equipment release to 423430 wholesalers) is left open without documentation.
8. Complete the closeout record: environmental status, backup status, open/escalated tickets, security confirmation, and exceptions; save to the operations log and queue for the OD-002 handover.

## 8. Decision Tree

OD-030 · OPERATIONS · DATA HOSTING

## Decision Tree — End-of-Shift / End-of-Day Operations Closeout




READING THIS TREE

- **No finding** — Activity stands. Complete the checklist and continue.
- **Minor** — Handled in place at task level; no escalation.
- **Major** — Supervisory decision required before the next stage.
- **Critical** — Activity halts on the spot; escalation is immediate.

## 9. Quality Checkpoints

- All environmental readings verified within threshold and alarms accounted for.
- Backup/replication completion confirmed and failures documented with job IDs.
- Ticket queue reconciled and escalations assigned to incoming shift.
- Zero unresolved Critical findings.

## 10. Inspection Checklist

| ITEM | PASS / FAIL | NOTES |
|---|---|---|
| Environmental readings within threshold; alarms recorded | | |
| Backup/replication jobs verified; failures documented | | |
| Ticket queue reconciled; escalations assigned | | |
| Rack doors, cages, and cabinets physically secured | | |
| Shared consoles/KVM logged out; privileged sessions closed | | |
| Inbound hardware/spares and media logged and stored | | |
| Closeout record completed and queued for handover (OD-002) | | |

## 11. KPIs

- Backup/replication verification completeness: 100% of scheduled jobs accounted for.
- Closeout record completed on time: ≥ 98% of operating periods.
- Unresolved Critical findings carried past close: 0.

## 12. Supervisor Verification

Printed Name: _____ Signature: _____ Date: _____

## 13. Revision History

| VERSION | DATE | DESCRIPTION | AUTHOR |
|---|---|---|---|
| 1.0 | 2026-07-27 | Generated to the locked 3-page Free/$99 Standard standard for DATA_HOSTING. | Archetype Content Team |